

FIFTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
Second Regular Session)

'11 SEP 14 P5:45

SENATE

RECEIVED BY:

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”**

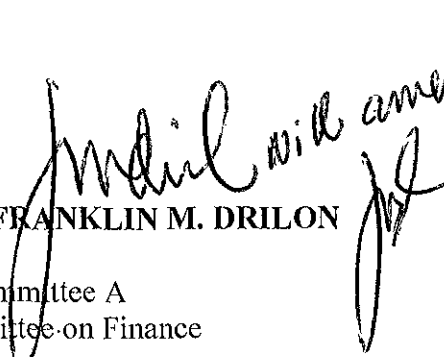
be approved in substitution of Senate Bill Nos. 355, 1908, ²⁹⁶⁵~~2836~~, taking into consideration House Bill No. 4115, with Senators Trillanes, Defensor Santiago and Angara as authors thereof.

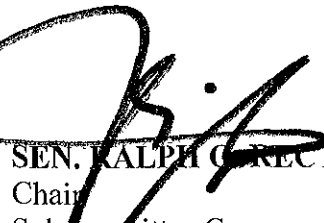
Respectfully submitted by:

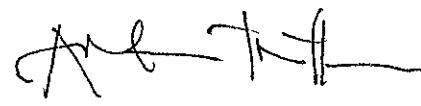
Chairpersons


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

Indial will amend.

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


SEN. RALPH RECTO
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



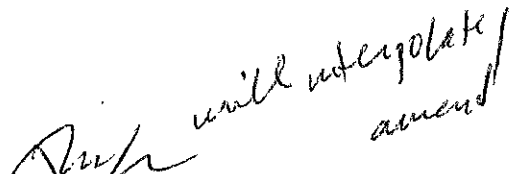
SEN. FERDINAND R. MARCOS, JR.
Member
Committee on Science & Technology
Committee on Constitutional Amendments,
Revision of Codes & Laws
Committee on Finance



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



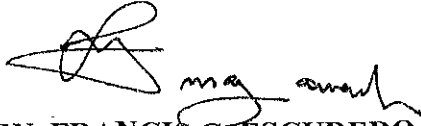
SEN. MANNY VILLAR
Member
Committee on Science & Technology
Committee on Constitutional Amendments,
Revision of Codes & Laws
Committee on Finance



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

Will introduce amendments

SEN. TEOFISTO L. GUINGONA III
Member
Committee on Finance

SEN. GREGORIO B. HONASAN
Member
Committee on Finance

Will Amend
A new 2

SEN. SERGIO R. OSMEÑA III
Member
Committee on Finance

SEN. RAMON REVILLA, JR.
Member
Committee on Finance

J. Arroyo, subject to amendments

SEN. JOKER P. ARROYO
Member
Committee on Finance

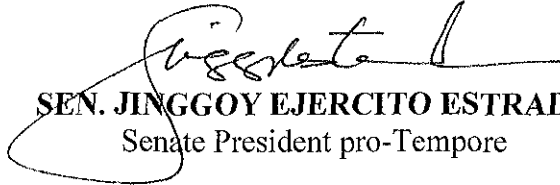
Pia S. Cayetano may interpellate/ amend.

SEN. PIA S. CAYETANO
Member
Committee on Finance


A. Pimentel may interpellate/ introduce amendments

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

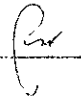
SEN. ALAN PETER S. CAYETANO
Senate Minority Floor Leader

SEN. JUAN PONCE ENRILE
Senate President
Pasay City

'11 SEP 14 P 6 :02

SENATE

S. No. 2965

RECEIVED BY: 

Prepared jointly by the Committees on Science and Technology; Constitutional Amendments, Revision of Codes and Laws; Civil Service & Govt. Reorg. and Finance with Senators Trillanes, Defensor-Santiago and Angara as authors

**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

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

4 **SEC. 2. *Declaration of Policy.***- It is the policy of the State to protect the
5 fundamental human right of privacy of communication. The State recognizes
6 the vital role of information and communications technology in nation-
7 building and its inherent obligation to ensure that personal information in
8 information and communications systems in the government and in the
9 private sector are secured and protected.

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

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

3 b.) **Consent of the data subject** refers to any freely given and informed
4 expression of will, either in written or electronic form executed personally and
5 voluntarily by the data subject, whereby the data subject agrees to the processing
6 of personal information about and/or relating to him or her.

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

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

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

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

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

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

31 1) A person or organization who performs such functions as instructed by
32 another person or organization; and

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

3 i.) **Personal information processor** refers to any operation or any set of
4 operations performed upon personal information including, but not limited
5 to, the collection, recording, organization, storage, updating or modification,
6 retrieval, consultation, use, consolidation, blocking, erasure or destruction of
7 data.

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

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

14 l.) **Sensitive personal information** refers to personal information:

15 (1) About an individual race, ethnic origin, color and religious,
16 philosophical or political affiliations;

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

21 (3) Issued by Philippine government agencies peculiar to an individual
22 which includes, but not limited to, Social Security numbers, previous or
23 current health records, licenses or its denials, suspension or revocation, and
24 tax returns; and

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

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

1 This Act does not apply to the following:

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

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

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

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

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

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

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

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

21 e) Information necessary in order to carry out the functions of public authority
22 which includes the processing of personal data for the performance by the
23 independent central monetary authority and law enforcement agencies of their
24 constitutionally and statutorily mandated functions.

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

4 **SEC. 5. Extraterritorial Application.** - This Act applies to an act done or practice
5 engaged in and outside of the Philippines by an entity if:

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

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

12 (1) A contract is entered in the Philippines;

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

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

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

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

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

21 **Chapter II. THE NATIONAL PRIVACY COMMISSION**

22 **SEC. 6. Functions of the National Privacy Commission** - To administer and
23 implement the provisions of this Act, and to monitor and ensure compliance of the
24 country with international standards set for data protection, there is hereby created an
25 independent body to be known as the National Privacy Commission, which shall have the
26 following functions:

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

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

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

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

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

20
21 (f) Recommend to the Department of Justice (DOJ) the prosecution and
22 imposition of penalties specified in Sec. 22 to 26 of This Act;

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

26 (h) Review, approve, reject or require modification of privacy codes voluntarily
27 adhered to by personal information controllers, provided that the privacy codes
28 shall adhere to the underlying data privacy principles embodied in this Act,
29 and provided further that such privacy codes may include private dispute

1 resolution mechanisms for complaints against any participating personal
2 information controller.

3 **SEC. 7. *Organizational Structure of the Commission.*** – The Commission shall
4 be attached to the Office of the President and shall be headed by a Privacy
5 Commissioner, who shall also act as Chairman of the Commission. The Privacy
6 Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be
7 responsible for Data Processing Systems and one to be responsible for Policies and
8 Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners
9 shall be appointed by the President of the Philippines for a term of three (3) years, and
10 may be reappointed for another term of three (3) years. Vacancies in the Commission shall
11 be filled in the same manner in which the original appointment was made.

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

17 The Deputy Privacy Commissioners must be recognized experts in the field of ICT
18 and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to
19 the rank of Undersecretary.

20 No criminal or civil proceedings shall lie against the Privacy Commissioner, the
21 Deputy Privacy Commissioners, or any person acting on their behalf or under their
22 direction, for anything done, reported or said in good faith as a result of the performance
23 or exercise or purported performance or exercise of any duty or power under this Act.

24 **SEC. 8. *The Secretariat.*** – The Commission is hereby authorized to establish a
25 Secretariat. Majority of the members of the Secretariat must have served for at least five
26 (5) years in any agency of the government that is involved in the processing of personal
27 information, Social Security System (SSS), Government Service Insurance System
28 (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine
29 Health Insurance Corporation (Philhealth), Commission on Elections (Comelec),

1 Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine
2 Postal Corporation (Philpost).

3 Chapter III. PROCESSING OF PERSONAL INFORMATION

4 **SEC. 9. General Data Privacy Principles.** - The processing of personal
5 information shall be allowed, subject to compliance with the requirements of this Act and
6 other laws allowing disclosure of information to the public and adherence to the
7 principles of transparency, legitimate purpose and proportionality.

8 Personal information must be:

- 9 (a) Collected for specified and legitimate purposes determined and declared
10 before, or as soon as reasonably practicable, and later processed in a way
11 compatible with such declared, specified and legitimate purposes only;
- 12 (b) Processed lawfully;
- 13 (c) Accurate, relevant, and, where necessary, for purposes for which it is to be
14 used the processing of personal information, kept up to date; inaccurate or
15 incomplete data must be rectified, supplemented, destroyed or their further
16 processing restricted;
- 17 (d) Adequate and not excessive in relation to the purposes for which they are
18 collected and processed;
- 19 (e) Retained only for as long as necessary for the fulfillment of the purposes
20 for which the data was obtained or for the establishment, exercise or
21 defense of legal claims, or for legitimate business purposes, or as provided
22 by law;
- 23 (f) Kept in a form which permits identification of data subjects for no longer
24 than is necessary for the purposes for which the data were collected and
25 processed: *Provided, further,* That adequate safeguards are guaranteed by
26 said laws authorizing their processing.

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

29 **SEC. 9-A. Principle of Accountability.** – Each personal information controller is
30 responsible under its control or custody, including information that have been transferred

1 to a third party for processing, whether domestically or internationally, subject to cross-
2 border arrangement and cooperation.

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

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

11 **SEC. 10. *Criteria for Lawful Processing of Personal Information.*** – The
12 processing of personal information shall be permitted only if not otherwise
13 prohibited by law, and when at least one of the following conditions exist:

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

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

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

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

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

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

30 **SEC. 11. *Sensitive Personal Information and Privileged Information.*** - The
31 processing of sensitive personal information and privileged information shall be
32 prohibited, except in the following cases:

1 (a) The data subject has given his or her express consent, specific to the
2 purpose prior to the processing;

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

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

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

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

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

25 **SEC. 12. *Subcontract of Personal Information.*** - A personal information
26 controller may subcontract the processing of personal information: *Provided*, That the
27 personal information controller shall be responsible for ensuring that proper safeguards
28 are in place to ensure the confidentiality of the "personal information, processed, prevent
29 its use for unauthorized purposes, and generally, comply with the requirements of this
30 Act and other laws for processing of personal information. The personal information
31 processor shall comply with all the requirements of this Act and other applicable laws.

32 **SEC. 13. *Storage of Data.*** – Personal information shall be stored and used only
33 for as long as it is necessary to achieve the purpose for which it was processed and all

1 related purposes, after which the personal information shall be deleted or blocked from a
2 personal information base, unless otherwise provided by law.

3 **SEC. 14. *Extension of Privileged Communication.*** – Personal information
4 controllers may invoke the principle of privileged communication over privileged
5 information that they lawfully control or process. Subject to existing laws and
6 regulations, any evidence gathered on privileged information is inadmissible.

7 **CHAPTER IV. RIGHTS OF THE DATA SUBJECT**

8 **SEC. 15. *Rights of the Data Subject.*** – The data subject is entitled to:

- 9 (a) Be informed whether personal information pertaining to him or her shall be,
10 are being or have been processed;
- 11 (b) Be furnished the information indicated hereunder before the entry of his or
12 her personal information into the processing system of the personal
13 information controller, or at the next practical opportunity;
- 14 (1) Description of the personal information to be entered into the system;
15 (2) Purposes for which they are being or are to be processed;
16 (3) Scope and method of the personal information processing;
17 (4) The recipients or classes of recipients to whom they are or may be
18 disclosed; and
19 (5) Methods utilized for automated access, if the same is allowed by the data
20 subject, and the extent to which such access is authorized.

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

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

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

3 (2) Sources from which personal information were obtained;

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

5 (4) Manner by which such data were processed;

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

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

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

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

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

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

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

4 **SEC. 16. *Transmissibility of Rights of the Data Subject.*** – The lawful heirs and
5 assigns of the data subject may invoke the rights of the data subject for which he or she
6 is an heir or assignee at any time after the death of the data subject or when the data
7 subject is incapacitated or incapable of exercising the rights as enumerated in the
8 immediately preceding section.

9 **SEC. 17. *Non-Applicability.*** – The immediately preceding sections are not
10 applicable if the processed personal information are used only for the needs of scientific
11 and statistical research and, on the basis of such, no activities are carried out and no
12 decisions are taken regarding the data subject: *Provided*, That the personal information
13 shall be held under strict confidentiality and shall be used only for the declared purpose.
14 Likewise, the immediately preceding sections are not applicable to processing of personal
15 information gathered for the purpose of investigations in relation to any criminal,
16 administrative or tax liabilities of a data subject.

17 **Chapter V. SECURITY OF PERSONAL INFORMATION**

18 **SEC. 18. *Security of Personnel Information.*** -

19 (a) The personal information controller must implement reasonable and
20 appropriate organizational, physical and technical measures intended for
21 the protection of personal information against any accidental or unlawful
22 destruction, alteration and disclosure, as well as against any other unlawful
23 processing.

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

29 (c) The determination of the appropriate level of security under this section
30 must take into account the nature of the personal information to be
31 protected, the risks represented by the processing, the size of the

1 organization and complexity of its operations, current data privacy best
2 practices and the cost of security implementation. Subject to guidelines as
3 the Commission may issue from time to time, the measures implemented
4 must include:

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

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

9 (3) A process for identifying and assessing reasonably foreseeable
10 vulnerabilities in its computer networks, and for taking preventive,
11 corrective and mitigating action against security incidents that can lead
12 to a security breach.

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

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

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

25 (f) The personal information controller shall promptly notify the Commission
26 and affected data subjects when sensitive personal information or other
27 information that may, under the circumstances, be used to enable identity
28 fraud are reasonably believed to have been acquired by an unauthorized
29 person, and the personal information controller or the Commission believes
30 that such unauthorized acquisition is likely to give rise to a real risk of
31 serious harm to any affected data subject. The notification shall at least
32 describe the nature of the breach, the sensitive personal information
33 possibly involved, and the measures taken by the entity to address the

1 breach. Notification may be delayed only to the extent necessary to
2 determine the scope of the breach, to prevent further disclosures, or to
3 restore reasonable integrity to the information and communications
4 system.

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

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

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

16 **Chapter VI. SECURITY OF SENSITIVE PERSONAL INFORMATION IN**
17 **GOVERNMENT**

18 **SEC. 19. *Responsibility of Heads of Agencies.*** - All sensitive personal
19 information maintained by the government, its agencies and instrumentalities shall be
20 secured, as far as practicable, with the use of the most appropriate standard recognized by
21 the information and communications technology industry, and as recommended by the
22 Commission. The head of each government agency or instrumentality shall be
23 responsible for complying with the security requirements mentioned herein while the
24 Commission shall monitor the compliance and may recommend the necessary action in
25 order to satisfy the minimum standards.

26 **SEC. 20. *Requirements Relating to Access by Agency Personnel to Sensitive***
27 ***Personal Information.*** -

28 (a) On-site and Online Access - Except as may be allowed through guidelines to
29 be issued by the Commission, no employee of the government shall have
30 access to sensitive personal information on government property or through

1 online facilities unless the employee has received a security clearance from the
2 head of the source agency.

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

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

13 (2) Limitation to One thousand (1,000) Records – If a request is approved,
14 the head of the agency shall limit the access to not more than one thousand
15 (1,000) records at a time; and

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

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

22 **SEC. 21. *Applicability to Government Contractors.*** - In entering into any
23 contract that may involve accessing or requiring sensitive personal information from one
24 thousand (1,000) or more individuals, any agency shall require a contractor and its
25 employees to register their personal information processing system with the Commission
26 in accordance with this Act and to comply with the other provisions of this Act including
27 the immediately preceding section, in the same manner as agencies and government
28 employees comply with such requirements.

1 **Chapter VII. PENALTIES**

2 **Sec. 22. *Unauthorized Processing of Personal Information and Sensitive***
3 ***Personal Information.* –**

4 a) The unauthorized processing of personal information shall be penalized
5 by imprisonment ranging from one (1) year to three (3) years and a fine of not
6 less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than
7 Two Million Pesos (Php2,000,000.00) shall be imposed on persons who
8 process personal information without the consent of the data subject, or
9 without being authorized under this Act or any existing law.

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

16 **SEC. 23. *Accessing Personal Information and Sensitive Personal***
17 ***Information Due to Negligence.* –**

18 a) Accessing Personal Information due to negligence shall be penalized by
19 imprisonment ranging from one (1) year to three (3) years and a fine of not less
20 than Five Hundred Thousand Pesos (Php 500,000.00) but not less or more than
21 Two Million Pesos (Php 2,000,000.00) shall be imposed on persons who, due to
22 negligence, provided access to personal information without being authorized
23 under this Act or any existing law.

24 b) Accessing Sensitive Personal Information due to negligence shall be penalized by
25 imprisonment ranging from three (3) years to six (6) years and a fine of not less
26 than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Four
27 Million Pesos (Php 4,000,000.00) shall be imposed on persons who, due to
28 negligence, provided access to personal information without being authorized
29 under this Act or any existing law.

1 **SEC. 24. *Improper Disposal of Personal Information and Sensitive Personal***
2 ***Information.*** –

- 3
- 4 a) The improper disposal of personal information shall be penalized by
5 imprisonment ranging from six (6) months to two (2) years and a fine not less
6 than One Hundred Thousand Pesos (Php 100,000.00) but not more than Five
7 Hundred Thousand Pesos (Php 500,000.00) shall be imposed on persons who
8 knowingly or negligently dispose, discard or abandon the personal information
9 of an individual in an area accessible to the public or has otherwise placed the
10 personal information of an individual in its container for trash collection.
- 11 b) The improper disposal of sensitive personal information shall be penalized by
12 imprisonment ranging from one (1) year to three (3) years and a fine not less
13 than One Thousand Pesos (Php 100,000.00) but not more than One Million
14 Pcsos (Php 1,000,000.00) shall be imposed on persons who knowingly or
15 negligently, dispose, discard or abandon the personal information of an
16 individual in an area accessible to the public or has otherwise placed the
17 personal information of an individual in its container for trash collection.

18 **SEC. 25. *Wrongful Processing of Personal Information and Sensitive Personal***
19 ***Information.***

- 20 a) The processing of personal information for unauthorized purposes shall be
21 penalized by imprisonment ranging from one (1) year and six (6) months to
22 five (5) years and a fine of not less than Five Hundred Thousand Pesos (Php
23 500,000.00) but not more than One Million Pesos (Php 1,000,000.00) shall be
24 imposed on persons processing personal information for purposes not
25 authorized by the data subject, or otherwise authorized under this Act or under
26 existing laws.
- 27 b) The processing of sensitive personal information for unauthorized purposes
28 shall be penalized by imprisonment ranging from two (2) years to seven (7)
29 years and a fine not less than Five Hundred Thousand Pesos (Php 500,000.00)
30 but not more than Two Million Pesos (Php 2,000,000.00) shall be imposed on
31 persons processing personal information for purposes not authorized by the
32 data subject, or otherwise authorized under this Act or under existing laws.

1 **SEC. 26. *Processing of Personal Information and Sensitive Personal***
2 ***Information for Unauthorized Purposes.*** - The processing of personal information for
3 unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and
4 six (6) months to five (5) years and a fine of not less than Five Hundred Thousand Pesos
5 (Php 500,000.00) but not more than One Million Pesos (Php 1,000,000.00) shall be
6 imposed on persons processing personal information for purposes not authorized by the
7 data subject, or otherwise authorized under this Act or under existing laws.

8a) The processing of sensitive personal information for unauthorized purposes shall be
9 penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of
10 not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Two
11 Million Pesos (Php 2,000,000.00) shall be imposed on persons processing personal
12 information for purposes not authorized by the data subject, or otherwise authorized
13 under this Act or under existing laws.

14
15 **SEC. 27. *Unauthorized Access or Intentional Breach.*** - The penalty of
16 imprisonment ranging from one (1) year to three (3) years and a fine not less than Five
17 Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php
18 2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating
19 data confidentiality and security data systems, breaks in any way into any system where
20 personal and sensitive personal information is stored.

21 **SEC. 28. *Concealment of Security Breaches Involving Sensitive Personally***
22 ***Identifiable Information.*** - The penalty of imprisonment of one (1) year and six (6)
23 months to five (5) years and a fine of not less than Five Hundred Thousand (Php
24 500,000.00) but not more than One Million Pesos (Php 1,000,000.00) shall be imposed
25 on persons who, after having knowledge of a security breach and of the obligation to
26 notify the Commission pursuant to Section 18 (f), intentionally or by omission conceals
27 the fact of such security breach.

28 **SEC. 29. *Malicious Disclosure.*** - Any person who, with malice or in bad faith,
29 discloses unwarranted or false information relative to any personal information or
30 personal sensitive information obtained by him or her from a data controller or
31 unknowingly transferred to him or her, shall be subject to imprisonment ranging from one
32 (1) year and six (6) months to five (5) years imprisonment and a fine of not less than Five

1 Hundred Thousand Pesos (Php 500,000.00) but not more than One Million Pesos (Php
2 1,000,000.00).

3 **SEC. 30. *Unauthorized Disclosure.* -**

- 4 a) Any person who discloses to a third party personal informal not covered by the
5 immediately preceding section without the consent of the data subject obtained by
6 him from a data controller or unknowingly transferred to him, shall be subject to
7 imprisonment ranging from one (1) year to three (3) years imprisonment and a fine
8 of not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than
9 One Million Pesos (Php 1,000,000.00).
- 10 b) Any person who discloses to a third party sensitive personal information not
11 covered by the immediately preceding section without the consent of the data
12 subject obtained by him from a data controller or unknowingly transferred to him,
13 shall be subject to imprisonment ranging from three (3) years to five (5) years
14 imprisonment and a fine of not less than Five Hundred Thousand Pesos (Php
15 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00).

16 **SEC. 31. *Breach of Confidentiality.* -** The penalty of imprisonment ranging from
17 two (2) years and four (4) months to five (5) years and a fine not less than Five Hundred
18 Thousand Pcsos (Php 500,000.00) but not more than Two Million Pesos (Php
19 2,000,000,000.00) shall be imposed in case of a breach of confidentiality where such
20 breach has resulted in the information being published or reported by media. In this case,
21 the responsible reporter, writer, president, publisher, manager and editor-in-chief shall be
22 liable under this Act.

23 **SEC. 32. *Combination of Series of Acts.* -** Any combination or series of acts as
24 defined in Section 23 to 30 shall make the person subject to imprisonment ranging from
25 three (3) years to six (6) years and a fine of not less than One Million Pesos (Php
26 1,000,000.00) but not more than Five Million Pesos (Php 5,000,000.00).

27 **SEC. 33. *Extent of Liability.* -** If the offender is a corporation, partnership or any
28 juridical person, the penalty shall be imposed upon the responsible officers, as the case
29 may be, who participated in, or by their gross negligence, allowed the commission of the
30 crime. If the offender is a juridical person, the court may suspend or revoke any of its
31 rights under this Act. If the offender is an alien, he shall, in addition to the penalties

1 herein prescribed, be deported without further proceedings after serving the penalties
2 prescribed. If the offender is a public official or employee and he is found guilty of acts
3 penalized under Section 24 and 25 of this Act, he or she shall, in addition to the penalties
4 prescribed herein, suffer perpetual or temporary absolute disqualification from office, as
5 the case may be.

6 **SEC. 34. *Large-Scale.*** – The maximum penalty in the scale of penalties
7 respectively provided for the preceding offenses shall be imposed when the personal
8 information of at least one hundred (100) persons is harmed, affected or involved as the
9 result of the above mentioned actions.

10 **SEC. 35. *Offense Committed by Public Officer.*** – When the offender or the
11 person responsible for the offense is a public officer as defined in the Administrative
12 Code of the Philippines in the exercise of his duties, an accessory penalty consisting in
13 the disqualification to occupy public offices for a term double the term of criminal
14 penalty imposed shall be applied.

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

Chapter VIII. MISCELLANEOUS PROVISIONS

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

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

23 **SEC. 39. *Reports and Information.*** - The Commission shall annually report to
24 the President and Congress on its activities in carrying out the provisions of this Act. The
25 Commission shall undertake whatever efforts it may determine to be necessary or
26 appropriate to inform and educate the public of data privacy, data protection and fair
27 information rights and responsibilities.

1 **SEC. 40. Appropriations Clause.** – The Commission shall be provided with an
2 initial appropriation of Twenty Million Pesos (Php 20,000,000.00) to be drawn from the
3 national government. Appropriations for the succeeding years shall be included in the
4 General Appropriations Act. It shall likewise receive Ten Million Pesos (Php
5 10,000,000.00) per year for five years upon implementation of this Act drawn from the
6 national government.

7 **SEC. 41. Transitory Period.** - Existing industries, businesses and offices affected
8 by the implementation of this Act shall be given one (1) year transitory period from the
9 effectivity of the IRR or such other period as may determined by the Commission, to
10 comply with the requirements of this Act.

11 **SEC. 42. Separability Clause.** - If any provision, or part hereof, is held invalid or
12 unconstitutional, the remainder of the law or the provision not otherwise affected shall
13 remain valid and subsisting.

14 **SEC. 43. Repealing Clause.** – The provision of Section 7 of Republic Act No.
15 9372, otherwise known as the “Human Security Act of 2007”, is hereby amended. All
16 other laws, decrees, executive orders, proclamations and administrative regulations or
17 parts thereof inconsistent herewith are hereby repealed or modified accordingly.

18 **SEC. 44. Effectivity Clause.** – This Act shall take effect fifteen (15) days after its
19 publication in at least two (2) national newspapers of general circulation.

20 Approved,