

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

9 MAR 16 2011

SENATE

S. NO. 3129

RECEIVED  
*[Signature]*

---

Introduced by Senator Antonio "Sonny" F. Trillanes IV

---

**EXPLANATORY NOTE**

We are currently living in an information-driven economy. The advancement in Information and Communications Technology (ICT) paved the way for this type of economy to flourish. However, our capability to participate in such economy depends on the level of infrastructure and economic policies currently present in our country. But it cannot be argued that our participation in the information economy will be most beneficial to our country as we strive for economic growth.

In today's technology, processes, workflows and functions can be modularized and easily distributed. Location is no longer fixed by proximity as entire functions and departments can be globally sourced. In the Philippines, Business Process Outsourcing (BPO) industry has contributed much to our economy. According to the National Statistical Coordination Board (NSCB), on the average from the First Quarter of 2004 to the Second Quarter of 2007, the BPO industry has increased our country's GDP growth by as much as 0.2 percentage points. The industry also generated as much as US\$ 2 billion in 2005, 48.2% higher from the US\$ 1.3 billion the industry generated in 2004.

In addition, based on the projections made by BOI-CICT-BPA/P, the BPO industry is expected to contribute more to the economy, as much as US\$12 billion in 2010. Total workforce for the industry is also expected to increase and may reach 1.1 million in the same year, translating to 982,300 new jobs generated, from only 100,500 in 2004. Increased local employment, skills development and investment, tax revenues and other collateral spending in the economy are some of the results brought about by the industry. However, countries from all over the world are competing to attract outsourcing services.

The Philippines clearly has an advantage in attracting these services. We have a lot of technically skilled graduates, we are very proficient in the English language, and we have prior experience dealing with big companies in the US. However, aside from basic infrastructure, skilled labor,

and cost of setting up business here, investors also consider the level of trust in how transferred information will be secured and used in our country.

This bill seeks to provide the needed framework in relation to the handling and treatment of sensitive and personal information in our country. It also establishes a National Data Privacy Commission that would regulate the use of this information. It is hoped that thru this legislation we will be able to earn the trust of investors and utilize them to propel our country's growth economically.

In view of the foregoing, immediate passage of this bill is earnestly sought.



ANTONIO "SONNY" F. TRILLANES IV  
Senator

9 MAR 16 PM 5:51

SENATE

S. NO. 3129

RECEIVED BY 

---

Introduced by Senator Antonio "Sonny" F. Trillanes IV

---

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 I. GENERAL PROVISIONS

1  
2  
3       **SECTION 1. *Short Title.*** – This Act shall be known as the “Data Privacy Act of 2009”.  
4

5       **SEC. 2. *Declaration of Policy.*** – It is the policy of the State to protect the fundamental  
6 human right of privacy of communication. The State likewise recognizes the vital role of  
7 information and communications technology building but with its inherent obligation to ensure  
8 that personal information in information and communications systems in the government and the  
9 private sector are secure and protected.  
10

11       **SEC. 3. *Interpretation.*** – Any doubt in the interpretation of any provision of this Act  
12 shall be interpreted in favor of the rights and interests of the individual whose private  
13 information is being processed.  
14

15       **SEC. 4. *Definition of Terms.*** – Whenever used in this Act, the following terms shall  
16 have the respective meanings hereafter set forth:  
17

18       “Personal information” – means any information, or an opinion, whether true or not and  
19 whether recorded in a material form or not, about an individual whose identity is apparent  
20 or can be reasonably ascertained from information or opinion, or when put together with  
21 other information would identify an individual.

1 “Personal information controller” – means a person or organization who controls the  
2 collection, holding, processing or use of personal information, including a person or  
3 organization who instructs another person or organization to collect, hold, process, use  
4 transfer or disclose personal information on his or her behalf. The term excludes:

5  
6 (a) a person or organization who performs such functions as instructed by another  
7 person or organization; and

8 (b) an individual who collects, holds, processes or uses personal information in  
9 connection with the individual’s personal, family or household affairs.

10  
11 “Processing” – shall mean any operation or any set of operations concerning personal  
12 information, including, but not limited to, the collection, recording, organization, storage,  
13 updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or  
14 destruction of data.

15  
16 “Filing system” – means any set of information relating to natural or juridical persons to  
17 the extent that, although the information is not processed by means of equipment  
18 operating automatically in response to instructions given for that purpose, the set is  
19 structured, either by reference to individuals or by reference to criteria relating to  
20 individuals, in such a way that specific information relating to a particular person is  
21 readily accessible.

22  
23 “Sensitive personal information” – means personal information –

24  
25 (a) which is likely to give rise to unlawful or arbitrary discrimination, which  
26 includes, but is not limited to, data which indicate the race, ethnic origin, marital  
27 status, age, color, religious, philosophical or political affiliations;

28 (b) which provide information as to the health, education, genetic or sexual life of a  
29 person, or to any proceeding for any offense committed or alleged to have been  
30 committed by such person, the disposal of such proceedings, or the sentence of  
31 any court in such proceedings;

32 (c) which are issued by government agencies peculiar to an individual which  
33 includes, but not limited to, Social Security numbers, previous or current health  
34 records, licenses or its denials, suspension, or revocation, and Tax returns;

1 (d) which have been specifically authorized under criteria established by an  
2 Executive Order or an Act of Congress to be kept classified in the interest of  
3 national defense or foreign policy.  
4

5 “Privileged data” – means any and all forms of data which under Section 24, Rule 120 of  
6 the Rules of Court and other pertinent laws, constitute privileged communication,  
7 specifically but not limited to those pertaining to communication exchanged in  
8 confidence between –

- 9  
10 (a) Husband and Wife;  
11 (b) Lawyer and Client;  
12 (c) Physician and Patient;  
13 (d) Publisher, Editor or Reporter and their Informant;  
14 (e) Parents and their Children.  
15

16 “Data subject” – means an individual whose personal information is processed.  
17

18 “Consent of the data subject” – means any freely given, specific and informed expression  
19 of will, either in written or electronic form executed personally and voluntarily by the  
20 data subject, whereby the data subject agrees to the processing of personal information  
21 about and/ or relating to him or her.  
22

23 “Direct marketing” – means communication by whatever means of any advertising or  
24 marketing material which is directed to particular individuals.  
25

26 “Information and Communications System” – means a system for generating, sending,  
27 receiving, storing or otherwise processing electronic data messages or electronic  
28 documents and includes the computer system or other similar device by or in which data  
29 is recorded or stored and any procedures related to the recording or storage of electronic  
30 data message or electronic document.  
31

32 “Commission” – shall refer to the National Privacy Commission created by virtue of this  
33 Act.  
34

35 **SEC. 5. Scope.** – This Act applies to the processing of all types of personal information,  
36 and to any natural and juridical person involved in personal information processing including

1 those personal information controllers who, although not found or established in the Philippines,  
2 uses equipment that are located in the Philippines, or those who maintain an office, branch or  
3 agency in the Philippines subject to the immediately succeeding section.

4  
5 This Act does not apply to the information and communications systems in which  
6 personal information are processed for personal or household and family purposes and where the  
7 personal information collected are not disclosed to other persons. Likewise, this Act shall not  
8 apply if personal information is processed for journalistic, artistic or literary purposes.

9  
10 **Chapter II. THE NATIONAL PRIVACY COMMISSION**

11  
12 **SEC. 6. *Functions of the National Privacy Commission*** – To administer and implement  
13 the provisions of this Act, and to monitor and ensure compliance of the country with  
14 international standards set for data protection, there is hereby created an independent body to be  
15 known as the National Privacy Commission, which shall have the following functions:

- 16  
17 (a) Ensure compliance of personal information controllers with the provisions of this  
18 Act;
- 19 (b) Receive complaints, institute investigations, facilitate or enable settlement of  
20 complaints through the use of alternative dispute resolution processes, adjudicate,  
21 award indemnity on matters affecting any personal information, prepare reports on  
22 disposition of complaints and resolution of any investigation it initiates, and, in cases  
23 it deems appropriate, publicize any such report, provided that in resolving any  
24 complaint or investigation (except where amicable settlement is reached by the  
25 parties), the Commission shall act as a collegial body. For this purpose, the  
26 Commission may be given access to personal information subject of any complaint  
27 and to collect the information necessary to perform its functions under this Act;
- 28 (c) Issue cease and desist orders, impose a temporary or permanent ban on the processing  
29 or personal information, upon finding that the processing will be detrimental to  
30 national security and public interest;
- 31 (d) Monitor the compliance of other government agencies or instrumentalities on their  
32 security and technical measures and recommend the necessary action in order to meet  
33 minimum standards for protection of personal information pursuant to this Act;
- 34 (e) Coordinate with other government agencies and the private sector on efforts to  
35 formulate and implement plans and policies to strengthen the protection of personal  
36 information in the country;

- 1 (f) Recommend to the Department of Justice (DOJ) the prosecution and imposition of  
2 penalties specified in Sec. 22 to 27 of this Act;
- 3 (g) Ensure proper and effective coordination with data privacy regulators in other  
4 countries and private accountability agents, and participate in international and  
5 regional initiatives for data privacy protection; and;
- 6 (h) Review, approve, reject or require modification of privacy codes voluntarily adhered  
7 to by personal information controllers, provided that the privacy codes shall adhere to  
8 the underlying data privacy principles embodied in this Act, and provided further that  
9 such privacy codes may include private dispute resolution mechanisms for complaints  
10 against any participating personal information controller.

11

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

20

21 The Privacy Commissioner must be a member of the Philippine Bar, at least thirty-five  
22 (35) years of age and of good moral character, unquestionable integrity and known probity,  
23 preferably with experience in Information Technology as recommended by the Commission on  
24 Information and Communications Technology. The Privacy Commissioner shall enjoy the  
25 benefits, privileges and emoluments equivalent to the rank of Secretary.

26

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

30

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

1           **SEC. 8. *The Secretariat.*** – The Commission is hereby authorized to establish a  
2 Secretariat. Majority of the members of the Secretariat must have served for at least five (5)  
3 years in any agency of the government that is involved in the processing of personal information,  
4 including, but not limited to the following offices: National Statistics Office (NSO), Social  
5 Security System (SSS), Government Service Insurance System (GSIS), Land Transportation  
6 Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation  
7 (PhilHealth), Commission on Elections (Comelec), Department of Foreign Affairs (DFA),  
8 Department of Justice (DOJ), and Philippine Postal Corporation (PhilPost).

9  
10                           **Chapter III. PROCESSING OF PERSONAL INFORMATION**

11  
12           **SEC. 9. *General Data Privacy Principles.*** – The processing of personal information shall  
13 be allowed, subject to compliance with the requirements of this Act and adherence to the  
14 principles of transparency, legitimate purpose and proportionality.

15  
16           Personal information must be:

- 17
- 18           (a) collected for specified and legitimate purposes determined and declared before  
19           collecting personal information and later processed in a way compatible with such  
20           declared, specified and legitimate purposes only;
  - 21           (b) processed accurately, precisely, fairly and lawfully;
  - 22           (c) accurate, relevant, and, where necessary for the processing of personal information,  
23           kept up to date; inaccurate or incomplete data must be rectified, supplemented,  
24           destroyed or their further processing must be restricted;
  - 25           (d) consistent, adequate and not excessive in relation to the purposes for which they are  
26           collected and processes;
  - 27           (e) kept within a period not exceeding the time within which the purposes for which the  
28           data was obtained would be achieved;
  - 29           (f) kept in a form which permits identification of data subject for no longer than is  
30           necessary for the purposes for which the data were collected and processed; Provided,  
31           that personal information collected for other purposes may be processed for historical,  
32           statistical or scientific purposes and in cases laid down in law may be stored for  
33           longer periods; Provided, further, that adequate safeguards are guaranteed by said  
34           laws authorizing their processing.



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

3  
4 **SEC. 10. *Criteria for Lawful Processing of Personal Information.*** – The processing of  
5 personal information shall be permitted only if not otherwise prohibited by law, and at least one  
6 of the following conditions exist:

- 7
- 8 (a) the data subject has given his or her unambiguous consent which must be given in  
9 writing, or through any other similar means of express consent, according to the  
10 circumstances;
  - 11 (b) the personal information is necessary and is a legal consequence of a contractual  
12 obligation of the data subject or in order to take steps at the request of the data subject  
13 prior to entering into a contract;
  - 14 (c) the processing is necessary to protect vitally important interests of the data subject,  
15 including life and health; or
  - 16 (d) the processing is necessary in order to respond to national emergency, to comply with  
17 the requirements of public order and safety, or to fulfill functions of public authority  
18 which necessarily includes the processing of personal information for the fulfillment  
19 of its mandate.
- 20

21 **SEC. 11. *Sensitive Data and Privileged Data.*** – The processing of sensitive personal  
22 information and privileged data shall be prohibited, except in the following cases:

- 23
- 24 (a) the data subject has given his or her consent prior to the processing, or in the case of  
25 privileged data, all parties to the exchange have given their consent prior to the  
26 processing;
  - 27 (b) the processing of the same is provided for by existing laws and regulations; Provided,  
28 that such regulatory enactments guarantee the protection of the sensitive personal  
29 information and the privileged data; and Provided further, that the consent of the data  
30 subjects are not required by the law, or regulation permitting the processing of  
31 sensitive personal information or the privileged data;
  - 32 (c) the processing is necessary to protect the life and health of the data subject or another  
33 person, and the data subject is not legally or physically able to express his or her  
34 consent prior to the processing;
  - 35 (d) processing is necessary to achieve the lawful, non-commercial objectives of public  
36 organizations and their associations; Provided, such processing is only confined and

1 related to the bona fide members of these organizations or their associations;  
2 Provided further, that the sensitive personal information are not transferred to third  
3 parties; and Provided finally, that consent of the data subject was obtained prior to  
4 processing;

5 (e) the processing is necessary for the purposes of medical treatment, is carried out by a  
6 medical practitioner or a medical treatment institution, and an adequate level of  
7 protection of personal information is endured; or

8 (f) the processing concerns such personal information as is necessary for the protection  
9 of lawful rights and interests of natural or legal persons in court proceedings.

10  
11 **SEC. 12. *Subcontract of Personal Information.*** – A personal information controller may  
12 subcontract the processing of personal information provided, that, the personal information  
13 controller shall be responsible for ensuring that proper safeguards are in place to ensure the  
14 confidentiality of the personal information processed, prevent its use for unauthorized purposes,  
15 and generally, comply with the requirements of this Act for processing of personal information.

16  
17 **SEC. 13. *Storage of Data.*** – Personal information shall be stored and used only for as  
18 long as it is necessary to achieve the purpose for which it was processed, after which the personal  
19 information shall be deleted or blocked from a personal information base, unless otherwise  
20 provided by law.

21  
22 **SEC. 14. *Extension of Privileged Communication.*** – Personal information controllers  
23 may invoke the principle of privileged communication over privileged data that they lawfully  
24 control or process. Subject to existing laws and regulations, any evidence gathered on privileged  
25 data is inadmissible.

#### 26 27 **Chapter IV. RIGHTS OF THE DATA SUBJECT**

28  
29 **SEC. 15. *Rights of the Data Subject.*** – The data subject is entitled to:

30  
31 (a) be informed whether personal information pertaining to him or her shall be, are being,  
32 or have been processed;

33 (b) before the entry of his or her personal information into the processing system of the  
34 data controller, be furnished the following:

35 i. description of the personal information to be entered into the system;

36 ii. purposes for which they are being or are to be processed;

- 1           iii. scope and method of the personal information processing;  
2           iv. recipients or classes of recipients to whom they are or may be disclosed; and  
3           v. methods utilized for automated access, if the same is allowed by the data  
4           subject, and the extent to which such access is authorized.

5  
6           Any information supplied or declarations made to the data subject on these  
7           matters shall not be amended without prior notification of data subject;

8  
9           (c) be given reasonable access to, upon demand, the following:

- 10  
11           i. contents of his/ her personal information that were processed;  
12           ii. source from which personal information were obtained;  
13           iii. names and addresses of recipients of the personal information;  
14           iv. manner by which such data were processed;  
15           v. reasons for the disclosure of the personal information to recipients;  
16           vi. information on automated processes where data will or is likely to be made  
17           as the sole basis for any decision significantly affecting or will affect the  
18           data subject;  
19           vii. date when his or her personal information concerning the data subject were  
20           last accessed and modified;  
21           viii. the designation, or name, or identity and address of the data controller.

22  
23           (d) dispute the inaccuracy or error in the personal information and have the data  
24           controller correct it immediately and accordingly. If the personal information has  
25           been corrected, the personal information controller shall ensure the accessibility of  
26           both the new and the retracted information and the simultaneous receipt of the new  
27           and the retracted information by recipients thereof;

28  
29           (e) suspend, withdraw or order the blocking, removal or destruction of his or her personal  
30           information from the data controller's filing system upon discovery and substantial  
31           proof that the personal information are incomplete, outdated, false, unlawfully  
32           obtained, used for unauthorized purposes, used for direct marketing purposes, unless  
33           expressly authorized, or are no longer necessary for the purposes for which they are  
34           collected. In this case, the personal information controller shall rectify the inaccuracy  
35           without delay and notify third parties who have previously received such processed

1 data. Likewise, the personal information controller shall indemnify the data subject  
2 for any damages sustained by the latter due to such inaccuracy.

3  
4 **SEC. 16. *Non-applicability.*** – The preceding section is not applicable if the processed  
5 data are used only for the needs of scientific and statistical research and, on the basis of such, no  
6 activities are carried out and no decisions are taken regarding the data subject. Provided, that the  
7 personal information shall be held under strict confidentiality and shall be used the same only for  
8 the declared purpose.

9  
10 **Chapter V. SECURITY OF DATA**

11  
12 **SEC. 17. *Security of Data*** –

13  
14 (a) The personal information controller must implement appropriate organizational and  
15 technical measures intended for the protection of personal information against any accidental or  
16 unlawful destruction, alteration, and disclosure as well as against any other unlawful processing.  
17 These measures must ensure a level of security appropriate to the nature of the data to be  
18 protected and the risks represented by the processing.

19 (b) The personal information controller shall implement appropriate measures to  
20 protect personal information against natural dangers, such as accidental loss or destruction and  
21 human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and  
22 contamination. These measures, specified in a written document or its equivalent, must be  
23 appropriate to the nature of the data to be protected and the risks represented by the processing.

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

29 (d) The personal information controller shall notify the Commission and affected data  
30 subjects when sensitive personal information or other information such as the name, address and  
31 unique identifiers of data subjects, are reasonably believed to have been acquired by an  
32 unauthorized person, and the personal information controller or the Commission believes that  
33 such unauthorized acquisition may give rise to a real risk of serious harm to any affected data  
34 subject.

- 1 i. In evaluating the risk of harm is sufficient to warrant notification, the adequacy of  
2 encryption of personal information and existence of good faith in the acquisition of  
3 personal information shall be considered.
- 4 ii. Commission may exempt a personal information controller from notification where,  
5 in its reasonable judgment, such notification would not be in the public interest or in  
6 the interests of the affected data subjects.
- 7

## 8 **Chapter VI. ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION**

9

10 **SEC. 18. *Principle of Accountability.*** – Each personal information controller is  
11 responsible for personal information under its control or custody, including information that has  
12 been transferred to a third party for processing, whether domestically or internationally subject to  
13 cross-border arrangement and cooperation.

14

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

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

21

## 22 **Chapter VII. SECURITY OF SENSITIVE DATA IN GOVERNMENT**

23

24 **SEC. 19. *Securing of Sensitive Data Maintained by the Government.*** – All sensitive  
25 data maintained by the government, its agencies and instrumentalities shall be secured, as far as  
26 practicable, with the use of the most appropriate standard recognized by the information and  
27 communications industry, and as recommended by the Commission on Information and  
28 Communications Technology. The head of each government agency or instrumentality shall be  
29 responsible for complying with the security requirements mentioned herein while the  
30 Commission shall monitor the compliance and may recommend the necessary action in order to  
31 satisfy the minimum standards.

32

33 **SEC. 20. *Requirements Relating to Access by Agency Personnel to Sensitive Data.*** –

34 (a) On-Site and On-Line Access – No employee of the government shall have access  
35 to sensitive data on Government property or through on-line facilities unless the employee has  
36 received a security clearance from the head of the source agency.

1 (b) Off-Site Access – Sensitive data maintained by an agency may not be transported  
2 or accessed from a location off Government property unless a request for such transportation or  
3 access is submitted and approved by the head of the agency provided that the following are  
4 followed:

5  
6 PROCEDURES –

- 7
- 8 i. Deadline for Approval or Disapproval – In the case of any request submitted to the  
9 head of an agency, such head of an agency shall approve or disapprove the request  
10 within two (2) business days after the date of submission of the request.
  - 11 ii. Limitation to 1,000 Records – If a request is approved, the head of the agency shall  
12 limit the access to not more than 1,000 records at a time.
  - 13 iii. Encryption – Any technology used to store, transport, or access sensitive data, for  
14 purposes of off-site access approved under this subsection, shall be secured by the use  
15 of the most secure encryption standard recognized by the Commission on Information  
16 and Communications Technology.
  - 17 iv. Implementation – The requirements of this subsection shall be implemented not later  
18 than six (6) months after the date of the enactment of this Act.

19  
20 **SEC. 21. *Applicability to Government Contractors.*** – In entering into any contract that  
21 may involve accessing or requiring sensitive personal information from one thousand (1,000) or  
22 more individuals, an agency shall require the contractor and employees of the contractor to  
23 register their data processing system to the Commission in accordance with this Act and to  
24 comply with the other provisions of this Act including the immediately preceding section, in the  
25 same manner as agencies and government employees comply with such requirements.

26  
27 **Chapter VIII. PENALTIES**

28  
29 **SEC. 22. *Unauthorized Processing of Personal Information.*** – The penalty of  
30 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five  
31 Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php  
32 2,000,000.00) shall be imposed on persons who process personal information without the  
33 consent of the data subject, or without being authorized under this Act or any existing law.

34  
35 **SEC. 23. *Accessing Personal Information Due to Negligence.*** - The penalty of  
36 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five

1 Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php  
2 2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal  
3 information without being authorized under this Act or any existing law.

4  
5 **SEC. 24. *Improper Disposal of Personal Information.*** - The penalty of imprisonment  
6 ranging from six (6) months to two (2) years and a fine not less than One Hundred Thousand  
7 Pesos (Php 100,000.00) but not more than Five Hundred Thousand Pesos (Php 500,000.00) shall  
8 be imposed on persons who knowingly or negligently, dispose, discard or abandon the personal  
9 information of an individual in an area accessible to the public or has otherwise placed the  
10 personal information of an individual in a container for trash collection.

11  
12 **SEC. 25. *Wrongful Processing of Personal Information.*** - The penalty of imprisonment  
13 ranging from six (6) months to two (2) years and a fine not less than One Hundred Thousand  
14 Pesos (Php 100,000.00) but not more than Five Hundred Thousand Pesos (Php 500,000.00) shall  
15 be imposed on persons who knowingly inserts or has false information inserted in a personal  
16 information file.

17  
18 **SEC. 26. *Processing of Personal Information for Unauthorized Purposes.*** - The  
19 penalty of imprisonment from one (1) year and six (6) months to five (5) years and a fine of not  
20 less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than One Million Pesos  
21 (Php 1,000,000.00) shall be imposed on persons processing personal information for purposes  
22 not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

23  
24 **SEC. 27. *Unauthorized Access or Intentional Breach.*** - The penalty of imprisonment  
25 ranging from one (1) year to three (3) years and a fine not less than Five Hundred Thousand  
26 Pesos (Php 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00) shall be  
27 imposed on persons who knowingly and unlawfully, or violating data confidentiality and security  
28 data systems, breaks in any way into any system where personal information is stored.

29  
30 **SEC. 28. *Concealment of Security Breaches Involving Sensitive Personally***  
31 ***Identifiable Information.*** - The penalty of imprisonment of one (1) year and six (6) months to  
32 five (5) years and a fine of not less than Five Hundred Thousand Pesos (Php 500,000.00) but not  
33 more than One Million Pesos (Php 1,000,000.00) shall be imposed on persons who, after having  
34 knowledge of a security breach and of the obligation to notify the Commission pursuant to  
35 Section 17 (d), intentionally or by omission conceals the fact of such security breach.

1           **SEC. 29. Malicious Disclosure.** – Any person who, with malice or in bad faith, discloses  
2 unwarranted or false information relative to any personal information obtained by him or her  
3 from a data controller or unknowingly transferred to him or her, shall be subject to imprisonment  
4 ranging from one (1) year and six (6) months to five (5) years imprisonment and a fine of not  
5 less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than One Million Pesos  
6 (Php 1,000,000.00).

7  
8           **SEC. 30. Unauthorized Disclosure.** – Any person who discloses to a third party personal  
9 information not covered by the immediately preceding section without the consent of the data  
10 subject obtained by him from a data controller or unknowingly transferred to him, shall be  
11 subject to imprisonment ranging from one (1) year to three (3) years imprisonment and a fine of  
12 not less than Five hundred Thousand Pesos (Php 500,000.00) but not more than One Million  
13 Pesos (Php 1,000,000.00).

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

20  
21           **SEC. 32. Combination or Series of Acts.** – Any combination or series of acts as defined  
22 in Sections 22 to 30 shall make the person subject to imprisonment ranging from three (3) years  
23 to six (6) years and a fine of not less than One Million Pesos (Php 1,000,000.00) but not more  
24 than Five Million Pesos (Php 5,000,000.00).

25  
26           **SEC. 33. Extent of Liability.** – If the offender is a corporation, association, partnership or  
27 any juridical person, the penalty shall be imposed upon the responsible officers, as the case may  
28 be, who participated in, or by their gross negligence, allowed the commission of the crime. If the  
29 offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If  
30 the offender is an alien, he shall, in addition to the penalties herein prescribed, be deported  
31 without further proceedings after serving the penalties herein prescribed. If the offender is a  
32 public official or employee and he is found guilty of acts penalized under Section 24 and 25 of  
33 this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or  
34 temporary absolute disqualification from office, as the case may be.





1 government. Appropriations for the succeeding years shall be included in the General  
2 Appropriations Act.

3

4 **SEC. 40. *Transitory Period.*** – Existing Industries, Businesses, and Offices affected by  
5 the implementation of this Act shall be given one (1) year transitory period from the, effectivity  
6 of this Act, to comply with the requirements of this Act.

7

8 **SEC. 41. *Separability Clause.*** – If any provision of this Act is held invalid, the other  
9 provisions not affected shall remain in full force and effect.

10

11 **SEC. 42. *Repealing Clause.*** – The provision of Section 7 of Republic Act No. 9372 is  
12 hereby amended. All other laws, decrees, executive orders, proclamations and administrative  
13 regulations, or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

14

15 **SEC. 43. *Effectivity Clause.*** – This Act shall take effect fifteen (15) days after the  
16 completion of its publication in the Official Gazette or in at least two (2) newspapers of general  
17 circulation.

Approved,