COMMITTEE REPORT NO. 1059

Submitted by the Committee on Information and Communications Technology on June 26, 2021.

Re: House Bill No. 9651

Recommending its approval in substitution of House Bills Numbered 1188 and 5612

Sponsors: Representatives Victor A. Yap, Michael L. Romero, Ph.D., and John Reynald M. Tiangco

Mr. Speaker:

The Committee on Information and Communications Technology to which were referred House Bill No. 1188 introduced by Rep. Michael L. Romero, Ph.D., entitled:

“AN ACT
AMENDING REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE “DATA PRIVACY ACT OF 2012”, TO ADOPT A MORE SYSTEMATIC, COMPREHENSIVE AND EFFECTIVE PROTECTION PROGRAM, TO FOSTER THE IMPOSITION OF ALL EXISTING POLICIES AND GUIDELINES, INCREASING ITS PENALTIES AND SANCTIONS, AND FOR OTHER PURPOSES”

and House Bill No. 5612 introduced by Rep. Victor A. Yap, entitled:

“AN ACT
AMENDING REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE “DATA PRIVACY ACT OF 2012”

has considered the same and recommends that the attached House Bill No. 9651, entitled:

“AN ACT
STRENGTHENING THE REGULATORY FRAMEWORK ON DATA PRIVACY PROTECTION, ALIGNING WITH INTERNATIONAL STANDARDS, CHALLENGES, AND OTHER CROSS-BORDER DATA PROCESSING CONCERNS, AMENDING FOR THE PURPOSE REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE “DATA PRIVACY ACT OF 2012”


Respectfully submitted:

VICTOR A. YAP
Chairperson
Committee on Information and Communications Technology

THE HONORABLE SPEAKER
HOUSE OF REPRESENTATIVES
Quezon City
AN ACT
STRENGTHENING THE REGULATORY FRAMEWORK ON DATA PRIVACY PROTECTION, ALIGNING WITH INTERNATIONAL STANDARDS, CHALLENGES, AND OTHER CROSS-BORDER DATA PROCESSING CONCERNS, AMENDING FOR THE PURPOSE REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE “DATA PRIVACY ACT OF 2012”

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

1 SECTION 1. Section 3 of Republic Act No. 10173 is hereby amended to read as follows:

“SEC. 3. Definition of Terms. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

xxx

(C) BIOMETRIC DATA REFERS TO PERSONAL DATA RESULTING FROM SPECIFIC TECHNICAL PROCESSING RELATING TO THE PHYSICAL, PSYCHOLOGICAL OR BEHAVIORAL CHARACTERISTICS OF A NATURAL
PERSON, WHICH ALLOW OR CONFIRM THE UNIQUE IDENTIFICATION OF THAT NATURAL PERSON, SUCH AS FACIAL IMAGES OR DACTYLOSCOPIC DATA.

[(c)] (D) Data subject refers to [an individual] A NATURAL PERSON whose personal [information] DATA 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 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) GENETIC DATA REFERS TO PERSONAL DATA RELATING TO THE INHERITED OR ACQUIRED GENETIC CHARACTERISTICS OF A NATURAL PERSON WHICH GIVES UNIQUE INFORMATION ABOUT THE PHYSIOLOGY OR THE HEALTH OF THAT NATURAL PERSON AND WHICH, IN PARTICULAR RESULTS FROM AN ANALYSIS OF A BIOLOGICAL SAMPLE FROM THE NATURAL PERSON IN QUESTION.

[(f)] (G) 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 which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.

(H) PERSONAL DATA REFERS TO ALL TYPES OF PERSONAL INFORMATION.

(I) PERSONAL DATA BREACH REFERS TO A BREACH OF SECURITY LEADING TO THE ACCIDENTAL OR UNLAWFUL DESTRUCTION, LOSS, ALTERATION, UNAUTHORIZED DISCLOSURE OF, OR ACCESS TO,
PERSONAL INFORMATION TRANSMITTED, STORED OR OTHERWISE PROCESSED.

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

[(h)] (K) **Personal information controller** refers to a NATURAL OR JURIDICAL person, [or organization who controls the collection, holding.] PUBLIC AUTHORITY, AGENCY OR OTHER ENTITY WHICH, ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES AND MEANS OF THE processing [or use] of personal [information] DATA, including a NATURAL OR JURIDICAL person [or organization] who instructs another NATURAL OR JURIDICAL person [or organization] to [collect, hold,] process, [use, transfer or disclose] personal [information] DATA. The term excludes:

xxx

[(i)] (L) **Personal information processor** refers to any natural or juridical person [qualified to act as such under this Act] to whom a personal information controller may outsource the processing of personal [information] DATA pertaining to a data subject.

[(j)] (M) **Processing** refers to any operation or any set of operations performed upon personal [information] DATA including the collection, recording, organization, storage, updating or modification, DISCLOSURE, 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 personal laws constitute privileged communication.]

[(l)] (N) **Sensitive personal information** refers to personal information:

1. About an individual’s [race] RACIAL or ethnic origin, [marital status, age, color, and religious] RELIGION, philosophical BELIEF, LABOR or political affiliations;
(2) About an individual’s health, genetic DATA, BIOMETRIC DATA FOR THE PURPOSE OF UNIQUELY IDENTIFYING A NATURAL PERSON, [or] sexual life, SEXUAL ORIENTATION of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) CONSISTING OF UNIQUE IDENTIFIERS issued by government agencies peculiar to an individual which includes IDENTIFICATION NUMBERS, social security numbers, previous or current health records, AND licenses [or its denials, suspension or revocation, and tax returns]; and

(4) Specifically established by LAW, REGULATION OR executive order [or an act of Congress] to be [kept] classified OR CONFIDENTIAL, INCLUDING THOSE THAT CONSTITUTES PRIVILEGED COMMUNICATION.”

SEC. 2. Section 4 of Republic Act No. 10173 is hereby amended to read as follows:

“SEC. 4. Scope. The Act shall apply to the processing of all types of personal [information and to] DATA IN INFORMATION AND COMMUNICATIONS SYSTEMS OR ANY FILING SYSTEM BY any natural and juridical person involved in personal [information] DATA processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: Provided, That the requirements of Section 6 of this Act are complied with.

THE REQUIREMENTS UNDER SECTIONS 12 AND 13 OF this Act [does] SHALL not apply to the PROCESSING OF THE following PERSONAL DATA RECOGNIZED AS SPECIAL CASES:

(A) PROCESSING OF INFORMATION FOR THE PURPOSE OF ALLOWING PUBLIC ACCESS TO INFORMATION THAT FALL WITHIN MATTERS OF PUBLIC CONCERN, PERTAINING TO:

[(a)] (1) Information about any individual who is or was an officer or employee of [a] THE government [institution] that relates to the position or functions [of the individual] OF THE OFFICER OR EMPLOYEE, including
[THOSE PERFORMING A SERVICE UNDER CONTRACT FOR A GOVERNMENT INSTITUTION IN SO FAR AS INFORMATION IS RELATED TO SUCH SERVICE; AND

[(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;]

(2) INFORMATION RELATING TO A BENEFIT OF A FINANCIAL NATURE CONFERRED ON AN INDIVIDUAL UPON THE DISCRETION OF THE GOVERNMENT, INCLUDING THE NAME OF THE INDIVIDUAL AND THE EXACT NATURE OF THE BENEFIT: PROVIDED, THAT THEY DO NOT INCLUDE BENEFITS GIVEN IN THE COURSE OF AN ORDINARY TRANSACTION OR AS A MATTER OF RIGHT;

[(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)] (B) Personal information processed for journalistic, artistic, OR literary purpose [or research purposes] IN ORDER TO UPHOLD FREEDOM OF SPEECH, EXPRESSION, OR THE PRESS;
(C) PROCESSING OF INFORMATION FOR RESEARCH PURPOSES, INTENDED FOR PUBLIC BENEFIT OR DEVELOPMENT OF KNOWLEDGE, SUBJECT TO THE REQUIREMENTS OF APPLICABLE LAWS, REGULATIONS, AND ETHICAL STANDARDS;
(e) (D) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

(f) (E) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; 

(g) (F) [Personal] THE PROCESSING PERTAINS TO information originally collected from residents of foreign jurisdictions BEING PROCESSED IN THE PHILIPPINES: PROVIDED, THAT THE PROCESSING IS in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws; [which is, being processed in the Philippines.]

(G) PROCESSING OF INFORMATION NECESSARY IN ORDER TO CARRY OUT THE FUNCTIONS OF PUBLIC AUTHORITIES, FOR INFORMATION SHARING NECESSARY IN THE INVESTIGATION AND PROSECUTION OF CHILD PORNOGRAPHY AND OTHER FORMS OF CHILD EXPLOITATION, TERRORISM AND TRAFFICKING IN PERSONS, IN ACCORDANCE WITH THEIR CONSTITUTIONALLY OR STATUTORILY MANDATED FUNCTION: PROVIDED, THAT PROTECTION OF FUNDAMENTAL FREEDOMS ARE GUARANTEED;

(H) PROCESSING OF INFORMATION BY COURTS ACTING IN THEIR JUDICIAL CAPACITY, IN ORDER TO SAFEGUARD THE INDEPENDENCE OF THE JUDICIARY IN THE PERFORMANCE OF ITS JUDICIAL TASKS;
(I) INFORMATION NECESSARY FOR THE AUDIT FUNCTIONS AND TO
SAFEGUARD THE INDEPENDENCE OF THE COMMISSION ON AUDIT
(COA) IN THE PERFORMANCE OF ITS CONSTITUTIONAL MANDATE, AS
WELL AS THOSE INFORMATION NECESSARY FOR DEPARTMENTS,
BUREAUS, OFFICES, AGENCIES, AND INSTRUMENTALITIES OF THE
NATIONAL GOVERNMENT, LOCAL GOVERNMENT UNITS,
GOVERNMENT-OWNED OR CONTROLLED CORPORATIONS, AND ALL
OTHER ENTITIES, INCLUDING PRIVATE ENTITIES AFFECTED BY OR
UNDER THE JURISDICTION OF THE COA, TO COMPLY WITH
PRESIDENTIAL DECREE 1445, OTHERWISE KNOWN AS THE
GOVERNMENT AUDITING CODE OF THE PHILIPPINES AND OTHER
APPLICABLE LAWS; AND

(J) PROCESSING OF INFORMATION BY A NATURAL PERSON FOR THE
PURPOSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY:
PROVIDED, THAT THE REASONABLE FREEDOM GRANTED BY THIS ACT
DOES NOT EXTEND TO PERSONAL INFORMATION CONTROLLERS OR
PERSONAL INFORMATION PROCESSORS, WHO REMAIN SUBJECT TO
THE REQUIREMENTS OF IMPLEMENTING SECURITY MEASURES FOR
PERSONAL DATA PROTECTION: PROVIDED, FURTHER, THAT THE
PROCESSING OF THE INFORMATION PROVIDED IN THE PRECEDING
PARAGRAPHS SHALL BE EXEMPTED FROM THE REQUIREMENTS OF
THE ACT ONLY TO THE MINIMUM EXTENT NECESSARY TO ACHIEVE
THE SPECIFIC PURPOSE, FUNCTION, OR ACTIVITY.”

SECTION. 3. Section 6 of the same Act is hereby amended to read as follows:

“SEC. 6. Extraterritorial Application. – This Act applies to an act done or
practice engaged in and outside of the Philippines by an entity if:

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

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

(1) A contract is entered in the Philippines;
(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and
(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:
   (1) The entity carries on business in the Philippines; and
   (2) The personal information was collected or held by an entity in the Philippines.

(A) THE NATURAL OR JURIDICAL PERSON INVOLVED IN THE PROCESSING OF PERSONAL INFORMATION IS FOUND OR ESTABLISHED IN THE PHILIPPINES;
(B) THE PROCESSING OF PERSONAL INFORMATION IS BEING DONE IN THE PHILIPPINES;
(C) THE PROCESSING OF PERSONAL INFORMATION RELATES TO A PHILIPPINE CITIZEN OR RESIDENT WHO IS IN THE PHILIPPINES, WHERE THE PROCESSING ACTIVITIES OF A NATURAL OR JURIDICAL PERSON OUTSIDE THE PHILIPPINES INVOLVES OFFERING OF GOODS OR SERVICES, OR MONITORING OF BEHAVIOR WITHIN THE PHILIPPINES; OR
(D) THE PROCESSING RELATES TO PERSONAL INFORMATION OF A PHILIPPINE CITIZEN OR A RESIDENT, AND THE ENTITY:
   1. USES OF EQUIPMENT LOCATED IN THE COUNTRY, OR MAINTENANCE OF AN OFFICE, BRANCH OR AGENCY IN THE PHILIPPINES FOR PROCESSING OF PERSONAL INFORMATION.
   2. HAS ENTERED INTO A CONTRACT WITH ANOTHER ENTITY IN THE PHILIPPINES;
3. IS A JURIDICAL ENTITY THAT IS NOT INCORPORATED IN THE PHILIPPINES BUT WHICH EXERCISES CENTRAL MANAGEMENT AND CONTROL OVER OPERATIONS IN THE COUNTRY;
4. HAS A BRANCH, AGENCY, OFFICE OR SUBSIDIARY IN THE PHILIPPINES AND HAS ACCESS TO PERSONAL INFORMATION;
5. CONDUCTS BUSINESS IN THE PHILIPPINES; OR
6. COLLECTS OR HOLDS PERSONAL INFORMATION IN THE PHILIPPINES.”

SECTION. 4. Section 7 of the same Act is hereby amended to read as follows:

“SEC. 7. Functions of the National Privacy Commission. – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, which shall have the following functions:

xxx

(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: PROVIDED, FURTHER, THAT THE COMMISSION SHALL HAVE PRIMARY JURISDICTION OVER CASES INVOLVING VIOLATIONS OF THIS ACT. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

(C) ISSUE SUMMONS, SUBPOENA AND SUBPOENA DUCES TECUM TO ANY PERSON TO COMPEL THEIR ATTENDANCE IN INVESTIGATIONS OR PROCEEDINGS BEFORE THE COMMISSION, AND TO HOLD AND
PUNISH FOR CONTEMPT THOSE WHO DISREGARD ORDERS OR WRITS ISSUED IN THE COURSE OF THESE PROCEEDINGS;

[(c) ] (D) 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, public interest, OR IF IT IS NECESSARY TO PRESERVE AND PROTECT THE RIGHTS AND FREEDOMS OF DATA SUBJECTS;

(E) IMPOSE ADMINISTRATIVE SANCTIONS, INCLUDING MONETARY PENALTIES FOR VIOLATIONS OF THE PROVISIONS THIS ACT, ITS IMPLEMENTING RULES AND REGULATIONS, AND ISSUANCES PURSUANT THERETO OR FOR FAILURE OR REFUSAL TO COMPLY WITH COMPLIANCE ORDERS AND RESOLUTIONS OF THE COMMISSION: PROVIDED, THAT THE COMMISSION MAY PROMULGATE FINES AND PENALTIES TAKING INTO CONSIDERATION THE ATTENDANT CIRCUMSTANCES, SUCH AS NATURE AND GRAVITY OF THE VIOLATION AND NUMBER OF AFFECTED DATA SUBJECTS;

[(d)] (F) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy, OR TO PROVIDE ASSISTANCE FOR THE EFFECTIVE IMPLEMENTATION OF THE ACT;

[(e)] (G) Monitor the compliance of [other government agencies or instrumentalities] PERSONAL INFORMATION CONTROLLERS AND PERSONAL INFORMATION PROCESSORS on their security and technical measures and recommend the necessary action in order to meet minimum standards for the protection of personal information pursuant to this Act;

[(f)] (H) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(I) CONDUCT SEMINARS, CONFERENCES AND TRAININGS FOR AWARENESS AND CAPACITY BUILDING IN RELATION TO ITS MANDATE;
[(g)] (J) Publish on a regular basis a guide to all laws relating to data
protection, AND PREPARE REPORTS ON DISPOSITION OF COMPLAINTS
AND RESOLUTION OF ANY INVESTIGATION IT INITIATES, AND, IN
CASES IT DEEMS APPROPRIATE, PUBLICIZE ANY SUCH REPORT;
[(h)] (K) Publish a compilation of agency system of records and notices,
including index and other finding aids;
[(i)] (L) Recommend to the Department of Justice (DOJ) the prosecution and
imposition of penalties specified in [Sections 25 to 29 of] this Act;
[(j)] (M) Review, approve, reject or require modification of privacy codes
voluntarily adhered to by personal information controllers: Provided, That the
privacy codes shall adhere to the underlying data privacy principles embodied
in this Act: Provided, further, That such privacy codes may include private
dispute resolution mechanisms for complaints against any participating
personal information controller. For this purpose, the Commission shall
consult with relevant regulatory agencies in the formulation and
administration of privacy codes applying the standards set out in this Act, with
respect to the persons, entities, business activities and business sectors that
said regulatory bodies are authorized to principally regulate pursuant to the
law: Provided, finally. That the Commission may review such privacy codes
and require changes thereto for purposes of complying with this Act;
[(k)] (N) Provide assistance on matters relating to privacy or data protection at
the request of a national or local agency, a private entity or any person;
[(l)] (O) Comment on the implication on data privacy of proposed national or
local statutes, regulations or procedures, issue advisory opinions and interpret
the provisions of this Act and other data privacy laws;
[(m)] (P) Propose legislation, amendments or modifications to Philippine laws
on privacy or data protection as may be necessary;
[(n)] (Q) Ensure proper and effective coordination with data privacy regulators
in other countries and private accountability agents, participate in
international and regional initiatives for data privacy protection;
[(o)] (R) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

[(p)] (S) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

[(q)](T) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection[,] IN ORDER TO PROTECT DATA SUBJECTS, AND TO ENSURE EFFECTIVE IMPLEMENTATION OF THIS ACT.”

SECTION 5. Section 9 of the same Act is hereby amended to read as follows:

“SEC. 9. Organizational Structure of the Commission. – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as [Chairman] CHAIRPERSON 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)] FOUR (4) years, and may be reappointed for another term of [three (3)] FOUR (4) years. Vacancies in the Commission shall be filled up in the same manner in which the original appointment was made: PROVIDED, THAT WHEN THE TERM OF A COMMISSIONER OR DEPUTY COMMISSIONER HAS EXPIRED AND NO ONE HAS YET BEEN APPOINTED TO THE VACANCY, THE COMMISSIONER OR DEPUTY COMMISSIONER, AS THE CASE MAY BE, SHALL CONTINUE TO PERFORM THE FUNCTIONS OF THE OFFICE IN A HOLD-OVER CAPACITY UNTIL A PERSON HAS BEEN APPOINTED TO SUCH POSITION: PROVIDED FURTHER, THAT IN CASE A VACANCY OCCURS BEFORE THE EXPIRATION OF THE TERM OF OFFICE OF ANY OF THE COMMISSIONERS OR DEPUTY COMMISSIONERS, THE APPOINTEE TO
SUCH VACANCY SHALL SERVE ONLY THE UNEXPIRED PORTION OF
THE TERM OF THE PREDECESSOR.

Xxx”

SECTION 6. Section 11 of the same Act is hereby amended to read as follows:

information shall be allowed, subject to compliance with the requirements of
the 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:

Xxx

(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, having regard to the purposes for which they are processed,
must be rectified, supplemented, destroyed or their further processing
restricted;

(d) Adequate, RELEVANT, and not excessive in relation to the purposes for
which they are collected and further processed;

Xxx

(f) Kept in a form which permits identification of data subjects for no longer
than is necessary for the purposes for which the data were collected and
processed: Provided, That personal information collected for other purposes
may be processed OR STORED LONGER SOLELY FOR ARCHIVING
PURPOSES IN THE PUBLIC INTEREST, for historical, statistical or
scientific purposes, and in cases laid down in law may be stored for longer
periods [: Provided, further, That adequate safeguards are guaranteed by said
laws authorizing their processing], SUBJECT TO IMPLEMENTATION OF
ADEQUATE SAFEGUARDS FOR DATA PROTECTION[.]; AND

(G) PROCESSED IN A MANNER THAT ENSURES APPROPRIATE
SECURITY OF THE PERSONAL INFORMATION.
The personal information controller must ensure implementation of personal information processing principles set out herein.”

SECTION 7. Section 12 of the same Act is hereby amended to read as follows:

“SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one (1) of the following conditions exists:

(a) The data subject has given consent: PROVIDED, THAT IN THE SPECIFIC CASE OF AN INFORMATION SOCIETY PROVIDER OFFERING SERVICES DIRECTLY TO A CHILD, THE PROCESSING OF THE PERSONAL INFORMATION OF A CHILD SHALL BE LAWFUL WHERE THE CHILD IS MORE THAN FIFTEEN (15) YEARS OLD. WHERE THE CHILD IS FIFTEEN (15) YEARS OLD OR BELOW, SUCH PROCESSING SHALL BE LAWFUL ONLY IF AND TO THE EXTENT THAT CONSENT IS GIVEN OR AUTHORIZED BY PERSONS EXERCISING PARENTAL AUTHORITY OVER THE CHILD;

(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;

Xxx

(d) The processing is necessary to protect vitally important interest of the data subject or OF ANOTHER NATURAL PERSON, including life and health;

Xxx”

SECTION 8. Section 13 of the same Act is hereby amended to read as follows:

“SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) WHEN the data subject has given consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing, EXCEPT IF A SPECIFIC LAW PROVIDES THAT THE PROHIBITION FROM PROCESSING MAY NOT BE LIFTED BY THE DATA SUBJECT;
(B) WHEN THE PROCESSING OF INFORMATION IS NECESSARY FOR THE
PERFORMANCE OF A CONTRACT FREELY ENTERED INTO BY THE
DATA SUBJECT AND PERSONAL INFORMATION CONTROLLER, OR IS
NECESSARY PURSUANT TO THE REQUEST OF A DATA SUBJECT
PRIOR TO ENTERING INTO A CONTRACT: PROVIDED, THAT THE
PERFORMANCE OF THE CONTRACT OR PROVISION OF THE SERVICE
IS NOT MADE CONDITIONAL ON THE DATA SUBJECT'S CONSENT TO
THE PROCESSING OF SENSITIVE PERSONAL INFORMATION THAT IS
NOT NECESSARY TO THE OBJECT OF THE CONTRACT;

[(b)] (C) WHEN THE [The] processing of the same is provided for by existing
laws and regulations: Provided, That such regulatory enactments OR THE
RULES ISSUED TO IMPLEMENT THEM guarantee the protection of [the]
sensitive personal information and [the] privileged information: Provided,
further, That the consent of the data subjects is not required by law or
regulation permitting the processing of the sensitive personal information;

[(c)] (D) WHEN THE [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 consent prior to the processing[;], OR WHEN: IN THE
INTEREST OF PUBLIC SAFETY, PROCESSING IS NECESSARY, SUCH AS
WHEN THE DATA SUBJECT IS A THREAT TO ONE'S SELF OR TO
OTHERS;

[(d)] (E) THE PROCESSING IS CARRIED OUT WITH APPROPRIATE
SAFEGUARDS BY A FOUNDATION, ASSOCIATION OR ANY OTHER NON-
PROFIT INSTITUTION WITH A CHARITABLE, RELIGIOUS,
PROFESSIONAL OR SIMILAR PURPOSE, IN THE COURSE OF ITS
LEGITIMATE ACTIVITIES AND ON CONDITION THAT THE PROCESSING RELATES SOLELY TO THE MEMBERS OR TO FORMER MEMBERS OF THE BODY, OR TO PERSONS WHO HAVE REGULAR CONTACT WITH IT IN CONNECTION WITH ITS PURPOSES, AND THAT THE PERSONAL INFORMATION IS NOT DISCLOSED OUTSIDE THAT BODY WITHOUT THE CONSENT OF THE DATA SUBJECTS;

[(e)] (F) The processing is necessary for the purpose of medical DIAGNOSIS AND treatment, PREVENTIVE OR OCCUPATIONAL MEDICINE, AND THE MANAGEMENT AND QUALITY ASSURANCE OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES, AND is carried out by a [medical practitioner or a medical treatment] HEALTH CARE institution, [and an adequate level of protection of personal information is ensured] HEALTH CARE PROVIDER, OR A PERSON UNDER THEIR RESPONSIBILITY WHO IS BOUND BY A PROFESSIONAL OR LEGAL OBLIGATION OF CONFIDENTIALITY, PROVIDED: THAT ADEQUATE SECURITY MEASURES ARE IMPLEMENTED FOR THE PROTECTION OF SENSITIVE PERSONAL INFORMATION;

(G) THE PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH OR HUMANITARIAN EMERGENCIES, PROVIDED: THAT SUCH PROCESSING IS COVERED BY OFFICIAL REGULATIONS ON PROCESSING AND IMPLEMENTATION OF APPROPRIATE SAFEGUARDS FOR DATA PROTECTION;

[(f)] (H) 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, WHENEVER COURTS ARE ACTING IN THEIR JUDICIAL CAPACITY, or the establishment, exercise or defense of legal claims IN CIVIL, CRIMINAL, ADMINISTRATIVE, AND OTHER SIMILAR PROCEEDINGS, [or] [when provided to government or public authority]; AND

(I) THE PROCESSING IS NECESSARY SOLELY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SUCH AS FOR SCIENTIFIC OR HISTORICAL RESEARCH OR STATISTICAL PURPOSES, TO THE EXTENT PROPORTIONATE TO THE AIM PURSUED AND CONSISTENT WITH
ETHICAL PRINCIPLES, WHICH SHALL PROVIDE FOR APPROPRIATE MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT.”

SECTION 9. Section 16 of the same Act is hereby amended to read as follows:

“SEC. 16. Rights of the Data Subject. – The data subject is entitled to the following rights:

(a) **RIGHT TO BE INFORMED.** The data subject shall be informed on whether personal information [pertaining to him or her] shall be, are being or have been processed, including intentions to further process the personal information for a purpose other than that for which the personal information were collected;

[(B)] the data subject shall be furnished provided the information indicated hereunder or where personal information is obtained from a third party before the entry of personal information into the processing system of the personal information controller, or [where personal information is obtained from a third party,] at the next practical opportunity:

1. Description of the personal information to be entered into the system;
2. The existence of automated decision-making, including profiling, as well as the significance and the envisaged consequences of such processing for the data subject;
3. (3) Purposes [for which they are being or are to be processed] and lawful basis of processing;
4. (4) Scope and method of the personal information processing;
5. Sources of personal information, and where applicable, whether it came from publicly accessible sources;
6. (6) The recipients or classes of recipients [to whom they are or may be disclosed] of personal information;
(5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

(7) TRANSFERS OR INTENDED TRANSFERS OF PERSONAL INFORMATION TO ANOTHER COUNTRY OR TO AN INTERNATIONAL ORGANIZATION;

[(6)] (8) The identity and contact details of the personal information controller or its representative;

(9) CONTACT DETAILS OF DATA PROTECTION OFFICER;

[(7)] (10) The period for which the information will be stored OR CRITERIA USED TO DETERMINE SUCH PERIOD; and

[(8)] (11) [The existence of their] THEIR rights as DATA SUBJECTS, to access[, correction,] AND CORRECT PERSONAL INFORMATION IN THE PROCESSING SYSTEM OF THE PERSONAL INFORMATION CONTROLLER, as well as the right to lodge a complaint before the Commission.

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

[(c) Reasonable access to, upon demand, the following:

Xxx

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

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

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

(B) RIGHT TO REASONABLE ACCESS. THE DATA SUBJECT HAS THE RIGHT TO REASONABLE ACCESS TO THE INFORMATION PROVIDED IN THE PRECEDING PARAGRAPH. THE DATA SUBJECT MAY OBTAIN A COPY OF THE PERSONAL INFORMATION UNDERGOING PROCESSING: PROVIDED, THAT THE RIGHT TO OBTAIN A COPY SHALL NOT ADVERSELY AFFECT THE RIGHTS AND FREEDOMS OF OTHERS.

(C) RIGHT TO OBJECT. THE DATA SUBJECT SHALL HAVE THE RIGHT TO OBJECT AT ANY TIME TO THE PROCESSING OF PERSONAL INFORMATION, ON GROUNDS RELATING TO A PARTICULAR SITUATION. THE DATA SUBJECT MAY OBJECT TO THE PROCESSING FOR DIRECT MARKETING PURPOSES, PROFILING OR TO HAVE DECISIONS MADE AFFECTING HIM OR HER BASED SOLELY ON AUTOMATED DECISION MAKING. THE PERSONAL INFORMATION CONTROLLER SHALL CEASE PROCESSING THE PERSONAL INFORMATION UNLESS THE CONTROLLER DEMONSTRATES COMPELLING LEGITIMATE GROUNDS FOR SUCH PROCESSING WHICH OVERRIDE THE INTERESTS, RIGHTS, AND FREEDOMS OF THE DATA
SUBJECT, OR FOR THE ESTABLISHMENT, EXERCISE OR DEFENSE OF
LEGAL CLAIMS.

THE DATA SUBJECT SHALL ALSO BE NOTIFIED AND GIVEN AN
OPPORTUNITY TO WITHHOLD CONSENT TO THE PROCESSING IN CASE
OF CHANGES OR ANY AMENDMENT TO THE INFORMATION SUPPLIED
OR DECLARED TO THE DATA SUBJECT IN THE PRECEDING
PARAGRAPHS.

WHEN A DATA SUBJECT OBJECTS OR WITHHOLDS CONSENT, THE
PERSONAL INFORMATION CONTROLLER SHALL NO LONGER PROCESS
THE PERSONAL INFORMATION, UNLESS THE PROCESSING IS
REQUIRED BY RELEVANT LAW AND REGULATION OR THE PROCESSING
FALLS IN ANY OF THE ALLOWABLE INSTANCES UNDER SECTIONS 4, 12
AND 13 OF THIS ACT.

(D) RIGHT TO RECTIFICATION. THE DATA SUBJECT HAS THE RIGHT TO
DISPUTE INACCURACY OR ERROR IN THE PERSONAL INFORMATION
AND HAVE THE PERSONAL INFORMATION CONTROLLER CORRECT IT
ACCORDINGLY WITHOUT DELAY, UNLESS THE REQUEST IS
VEXATIOUS OR OTHERWISE UNREASONABLE. IF THE PERSONAL
INFORMATION HAS BEEN CORRECTED, THE PERSONAL INFORMATION
CONTROLLER SHALL ENSURE THE ACCESSIBILITY OF BOTH THE NEW
AND THE RETRACTED INFORMATION AND THE SIMULTANEOUS
RECEIPT OF THE NEW AND THE RETRACTED INFORMATION BY
RECIPIENTS THEREOF: PROVIDED, 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.

TAKING INTO ACCOUNT THE PURPOSES OF THE PROCESSING, THE
DATA SUBJECT SHALL HAVE THE RIGHT TO PROVIDE ADDITIONAL
PERSONAL INFORMATION INCLUDING BY MEANS OF PROVIDING A
SUPPLEMENTARY STATEMENT.
(E) **RIGHT TO ERASURE.** THE DATA SUBJECT SHALL HAVE THE RIGHT TO SUSPEND OR RESTRICT PROCESSING, OR ORDER THE BLOCKING, REMOVAL OR DESTRUCTION OF PERSONAL INFORMATION FROM THE PERSONAL INFORMATION CONTROLLER'S FILING SYSTEM, WHERE:

1) THE PERSONAL INFORMATION IS INCOMPLETE, OUTDATED, FALSE, OR UNLAWFULLY OBTAINED;

2) THE PERSONAL INFORMATION IS BEING USED FOR PURPOSE NOT AUTHORIZED BY THE DATA SUBJECT;

3) THE PERSONAL INFORMATION IS NO LONGER NECESSARY FOR THE PURPOSES FOR WHICH IT WAS COLLECTED OR AS REQUIRED BY LAW;

4) THE DATA SUBJECT WITHDRAWS CONSENT OR OBJECTS TO THE PROCESSING, AND THERE IS NO OTHER LEGAL GROUND OR OVERRIDING LEGITIMATE INTEREST FOR THE PROCESSING;

5) THE PERSONAL INFORMATION CONCERNS PRIVATE INFORMATION THAT IS PREJUDICIAL TO DATA SUBJECT, UNLESS JUSTIFIED BY FREEDOM OF SPEECH, EXPRESSION, OR THE PRESS OR OTHERWISE AUTHORIZED;

6) THE PROCESSING IS UNLAWFUL; OR

7) THE PERSONAL INFORMATION CONTROLLER OR PERSONAL INFORMATION PROCESSOR VIOLATED THE RIGHTS OF THE DATA SUBJECT.

THE PERSONAL INFORMATION CONTROLLER MAY NOTIFY THIRD PARTIES WHO HAVE PREVIOUSLY RECEIVED SUCH PROCESSED PERSONAL INFORMATION; AND

(F) **RIGHT TO CLAIM DAMAGES.** THE DATA SUBJECT HAS THE RIGHT TO BE INDEMNIFIED FOR ANY DAMAGE SUSTAINED DUE TO SUCH INACCURATE, INCOMPLETE, OUTDATED, FALSE, UNLAWFULLY OBTAINED OR UNAUTHORIZED USE OF PERSONAL INFORMATION.”

SECTION 10. Section 19 of the same Act is hereby amended to read as follows:
“SEC. 19. [Non-applicability] LIMITATION ON RIGHTS OF DATA SUBJECTS. – The [immediately preceding sections are not applicable] RIGHTS OF DATA SUBJECT MAY BE LIMITED if the processed personal information IS [are] used only for the needs of scientific and statistical research, ARCHIVING PURPOSES IN THE PUBLIC INTEREST, 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] ADEQUATE SAFEGUARDS ARE IN PLACE and THE PERSONAL INFORMATION shall be used only for the declared purpose. [Likewise, the immediately preceding sections are not applicable to the] THE LIMITATION ALSO APPLIES WHEN SPECIFICALLY PROVIDED BY LAW, OR REGULATION, WHEN NECESSARY TO PROTECT LIFE AND HEALTH OF DATA SUBJECTS, OR WHERE THE processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.”

SECTION 11. Section 20 of the same Act is hereby amended to read as follows:


 X

 (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] WITHIN SEVENTY-TWO (72) HOURS UPON BEING AWARE OF OR UPON REASONABLE BELIEF THAT A PERSONAL DATA BREACH INVOLVING SENSITIVE PERSONAL INFORMATION OR OTHER INFORMATION THAT MAY BE USED TO ENABLE IDENTITY FRAUD OCCURRED. The notification shall at least describe the nature of the breach, the [sensitive] personal information possibly involved, and the measures taken by the [entity]
PERSONAL INFORMATION CONTROLLER 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.] WHERE SUCH
NOTIFICATION CANNOT BE ACHIEVED WITHIN SEVENTY-TWO (72)
HOURS, THE REASONS FOR THE DELAY SHOULD ACCOMPANY
THE NOTIFICATION AND INFORMATION MAY BE PROVIDED IN
PHASES WITHOUT ANY FURTHER DELAY.

[(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)] (1) The Commission may exempt a personal information controller from
notification NOTIFYING THE DATA SUBJECT where, in its reasonable
judgment, such notification would not be in the public interest or in the
interests of the affected data subjects. IN EVALUATING IF NOTIFICATION
IS UNWARRANTED, THE COMMISSION MAY TAKE INTO ACCOUNT
COMPLIANCE BY THE PERSONAL INFORMATION CONTROLLER WITH
THIS ACT AND EXISTING SECURITY MEASURES SHOWING THAT THE
PERSONAL DATA BREACH IS UNLIKELY TO RESULT IN A RISK TO
THE RIGHTS AND FREEDOMS OF NATURAL PERSONS.

[(3)] (2) The Commission may authorize postponement of notification where it
may hinder the progress of a criminal investigation related to a serious
breach. NOTIFICATION OF DATA SUBJECTS MAY BE DELAYED ONLY
TO THE EXTENT NECESSARY TO DETERMINE THE SCOPE OF THE
BREACH, PREVENT FURTHER DISCLOSURES, OR RESTORE
REASONABLE INTEGRITY TO THE INFORMATION AND
COMMUNICATIONS SYSTEM. WHERE THE PERSONAL DATA BREACH
IS LIKELY TO RESULT IN A HIGH RISK TO THE RIGHTS AND
FREEDOMS OF THE DATA SUBJECT, THE CONTROLLER SHOULD
COMMUNICATE TO THE DATA SUBJECT THE PERSONAL DATA
BREACH WITHOUT UNDUE DELAY, IN ORDER FOR THE DATA SUBJECT TO TAKE THE NECESSARY PRECAUTIONS.

FOR PURPOSES OF THIS SECTION, THE PERSONAL INFORMATION PROCESSOR WILL PROMPTLY REPORT TO THE PERSONAL INFORMATION CONTROLLER THE OCCURRENCE OF A PERSONAL DATA BREACH TO ALLOW FOR NOTIFICATION OF THE COMMISSION AND DATA SUBJECTS WITHIN THE PRESCRIBED PERIOD. IF THE PERSONAL INFORMATION CONTROLLER IS OUTSIDE THE PHILIPPINES AND IS UNABLE TO COMPLY WITH THE NOTIFICATION REQUIREMENTS, THE PERSONAL INFORMATION CONTROLLER MAY AUTHORIZE THE PERSONAL INFORMATION PROCESSOR, OR ANY OTHER THIRD PARTY, IN WRITING, TO SUBMIT THE BREACH NOTIFICATION TO THE COMMISSION, ON BEHALF OF THE PERSONAL INFORMATION CONTROLLER.”

SECTION 12. Section 21 of the same Act is hereby amended to read as follows:

“SEC. 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

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

b) The personal information controller shall designate A DATA PROTECTION OFFICER or an individual or individuals who are accountable for the organization’s compliance with THE PROVISIONS OF this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.”

SECTION 13. Section 24 of the same Act is hereby amended to read as follows:
“SEC. 24. Applicability to Government Contractors. ACCESS TO PERSONAL INFORMATION BY INDEPENDENT CONTRACTORS, CONSULTANTS, OR SERVICE PROVIDERS ENGAGED BY A GOVERNMENT AGENCY SHALL BE GOVERNED BY STRICT PROCEDURES CONTAINED IN FORMAL CONTRACTS, WHICH PROVISIONS MUST COMPLY WITH THE ACT. In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.”

SECTION 14. Section 25 of the same Act is hereby amended to read as follows:

“SEC. 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons] - ANY PERSON who SHALL process personal information without ANY LAWFUL [the consent of the data subject,] or without being authorized under this Act or any existing law SHALL BE PENALIZED BY IMPRISONMENT RANGING FROM ONE (1) YEAR TO THREE (3) YEARS OR A FINE OF NOT LESS THAN FIVE HUNDRED THOUSAND PESOS (PHP500,000.00) BUT NOT MORE THAN TWO MILLION PESOS (PHP2,000,000.00), OR BOTH.

(b) The unauthorized processing of personal sensitive information shall be penalized by] THE PENALTY OF imprisonment ranging from three (3) years to six (6) years [and] OR a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00), OR BOTH, 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.] IF SUCH UNAUTHORIZED PROCESSING INVOLVES SENSITIVE PERSONAL INFORMATION.”

SECTION 15. Section 26 of the same Act is hereby amended to read as follows:

“SEC. 26. PROVIDING ACCESS TO [Accessing] Personal Information and Sensitive Personal Information Due to Negligence. – [(a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons] ANY PERSON who, due to GROSS negligence, provided access to personal information without being authorized under this Act or any existing law SHALL BE PENALIZED BY IMPRISONMENT RANGING FROM ONE (1) YEAR TO THREE (3) YEARS OR A FINE OF NOT LESS THAN FIVE HUNDRED THOUSAND PESOS (PHP500,000.00) BUT NOT MORE THAN TWO MILLION PESOS (PHP2,000,000.00), OR BOTH.

[(b) Accessing sensitive personal information due to negligence shall be penalized by] THE PENALTY OF imprisonment ranging from three (3) years to six (6) years [and] OR a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00), OR BOTH shall be imposed [on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law] IF SUCH UNAUTHORIZED ACCESS INVOLVES SENSITIVE PERSONAL INFORMATION.”

SECTION 16. Section 27 of the same Act is hereby amended to read as follows:

“SEC. 27. Improper Disposal. – [of Personal Information and Sensitive Personal Information. – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons] ANY PERSON who knowingly or negligently disposeS[,]

OR discardS [or abandon the] personal information of an individual in [an] A
PHYSICAL area OR ONLINE PLATFORM accessible to the public [or has otherwise placed the personal information of an individual in its container for trash collection.] SHALL BE PENALIZED BY IMPRISONMENT RANGING FROM SIX (6) MONTHS TO TWO (2) YEARS OR A FINE OF NOT LESS THAN ONE HUNDRED THOUSAND PESOS (PHP100,000.00) BUT NOT MORE THAN FIVE HUNDRED THOUSAND PESOS (PHP500,000.00), OR BOTH.

[(b) The improper disposal of sensitive personal information shall be penalized by] THE PENALTY OF imprisonment ranging from one (1) year to three (3) years [and] OR a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00), OR BOTH 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.] IF SUCH IMPROPERLY DISPOSED OR DISCARDED DOCUMENTS CONTAIN SENSITIVE PERSONAL INFORMATION.”

SECTION 17. Section 28 of the same Act is hereby amended to read as follows:

“SEC. 28. Processing [of Personal Information and Sensitive Personal Information] for Unauthorized Purposes. – [The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons] ANY PERSON WHO, HAVING ACCESS TO PERSONAL INFORMATION, SHALL process[ing] SUCH personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws SHALL BE PENALIZED BY IMPRISONMENT RANGING FROM ONE (1) YEAR AND SIX (6) MONTHS TO FIVE (5) YEARS OR A FINE OF NOT LESS THAN FIVE HUNDRED THOUSAND PESOS (PHP500,000.00) BUT NOT MORE THAN ONE MILLION PESOS (PHP1,000,000.00), OR BOTH.
[The processing of sensitive personal information for unauthorized purposes shall be penalized by THE PENALTY OF imprisonment ranging from two (2) years to seven (7) years [and] OR a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00), OR BOTH shall be imposed [on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws] IF SUCH PROCESSING FOR UNAUTHORIZED PURPOSE INVOLVES SENSITIVE PERSONAL INFORMATION."

SECTION 18. Section 29 of the same Act is hereby amended to read as follows:

“SEC. 29. Unauthorized Access or Intentional Breach. – [The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons] ANY PERSON who knowingly and unlawfully, or violating [data] confidentiality [and] OR security OF data systems, breaks in any way into any system where personal [and] OR sensitive personal information is stored SHALL BE PENALIZED BY IMPRISONMENT RANGING FROM ONE (1) YEAR TO THREE (3) YEARS OR A FINE OF NOT LESS THAN FIVE HUNDRED THOUSAND PESOS (PHP500,000.00) BUT NOT MORE THAN TWO MILLION PESOS (PHP2,000,000.00), OR BOTH.”

SECTION 19. Section 30 of the same Act is hereby amended to read as follows:

“SEC. 30. Concealment of [Security] PERSONAL DATA Breaches [Involving Sensitive Personal Information. – The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on] - ANY person[s] who, after having knowledge of a [security] PERSONAL DATA breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such [security] PERSONAL DATA breach SHALL BE
PENALIZED BY IMPRISONMENT OF ONE (1) YEAR AND SIX (6) MONTHS TO FIVE (5) YEARS OR A FINE OF NOT LESS THAN FIVE HUNDRED THOUSAND PESOS (PHP500,000.00) BUT NOT MORE THAN ONE MILLION PESOS (PHP1,000,000.00), OR BOTH.”

SECTION 20. Section 31 of the same Act is hereby amended to read as follows:

“SEC. 31. Malicious Disclosure. – Any personal information controller or personal information processor or PERSONAL INFORMATION CONTROLLER or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or [personal] sensitive PERSONAL information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years [and] OR a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00), OR BOTH.”

SECTION 21. Section 32 of the same Act is hereby amended to read as follows:

“SEC. 32. Unauthorized Disclosure. – [(a)]Any personal information controller or personal information processor or PERSONAL INFORMATION CONTROLLER or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without [the consent of the data subject] BEING AUTHORIZED UNDER THIS ACT OR ANY EXISTING LAW, shall be subject to imprisonment ranging from one (1) year to three (3) years [and] OR a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00), OR BOTH.

[(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to] THE PENALTY OF imprisonment ranging from three (3) years to five (5) years [and] OR a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00), OR BOTH SHALL BE
SECTION 22. Section 33 of the same Act is hereby amended to read as follows:

“SEC. 33. Combination or Series of Acts. – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years [and] OR a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00), OR BOTH.”

SECTION 23. Section 34 of the same Act is hereby amended to read as follows:

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

SECTION 24. Section 36 of the same Act is hereby amended to read as follows:

“SEC. 36. Offense Committed by Public Officer. – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines COMMITS THE OFFENSE DURING [in] the exercise of [his or her] ONE’S duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied.

LIKEWISE, THE PUBLIC OFFICER, WHETHER SERVING IN A CASUAL, TEMPORARY, HOLDOVER, OR PERMANENT CAPACITY FOUND TO HAVE COMMITTED THE OFFENSE WILL BE SUBJECT TO ADMINISTRATIVE PENALTIES UNDER THE REPUBLIC ACT NO. 6713, OTHERWISE KNOWN
AS THE “CODE OF CONDUCT AND ETHICAL STANDARDS FOR PUBLIC OFFICIALS AND EMPLOYEES.”

SECTION 25. Section 37 of the same Act is hereby amended to read as follows:


AFTER DUE NOTICE AND HEARING, THE COMMISSION SHALL IMPOSE SANCTIONS, INCLUDING ADMINISTRATIVE FINES, WARNING OR REPRIMAND, UPON ANY PERSON FOR THE VIOLATION OF THE PROVISIONS OF THIS ACT, THE RULES AND REGULATIONS ISSUED TO IMPLEMENT IT, OR FOR FAILURE OR REFUSAL TO COMPLY WITH NPC ORDERS, RESOLUTIONS AND OTHER ISSUANCES.

[Restitution for any aggrieved party shall be governed] IN AWARDING OF CIVIL INDEMNITY TO DATA SUBJECTS AND PROVIDING RESTITUTION TO THE AGGRIEVED PARTY, THE COMMISSION SHALL BE GUIDED by the provisions of the New Civil Code.

THE IMPOSITION OF THE ADMINISTRATIVE SANCTIONS OR AWARD OF CIVIL INDEMNITY SHALL BE WITHOUT PREJUDICE TO THE FILING OF CRIMINAL CHARGES AGAINST THE PERSONS RESPONSIBLE FOR THE VIOLATION.”

SECTION 26. 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.

SECTION 27. Repealing Clause. – All other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.
SECTION 28. Effectivity. – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,
FACT SHEET

House Bill No. 9651
(in substitution of House Bills Numbered 1188 and 5612)

AN ACT
STRENGTHENING THE REGULATORY FRAMEWORK ON DATA PRIVACY PROTECTION, ALIGNING WITH INTERNATIONAL STANDARDS, CHALLENGES, AND OTHER CROSS-BORDER DATA PROCESSING CONCERNS, AMENDING FOR THE PURPOSE REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE “DATA PRIVACY ACT OF 2012”


Committee Referral: COMMITTEE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY

Committee Chairperson: REP. VICTOR A. YAP

OBJECTIVES

- To strengthen the implementation of the Data Privacy Act (DPA) and align it with the international standards on data privacy and protection.

- To affirm definitive functions of the National Privacy Commission (NPC) in the exercise of its quasi-judicial powers and in the effective enforcement of its orders so as to improve the application of the DPA.

- To cultivate a culture of privacy and to strengthen the DPA wherein government initiatives should take into consideration those that will involve processing of personal data, business models capitalizing on use of personal information, and emerging threats to data protection.

- To effectively address data privacy challenges and other cross-border data processing concerns in support of the country’s digital transformation towards a knowledge-based economy.
KEY PROVISIONS

- Provides clear-cut definition in the DPA for sensitive personal information of an individual as:
  - racial or ethnic origin, religious, philosophical belief, labor or political affiliations;
  - health, genetic data, biometric data for the purpose of uniquely identifying a natural person, sexual life, sexual orientation of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
  - financial data used by institutions whether or not regulated by the Bangko Sentral ng Pilipinas, for authenticating or verifying the identity of such individual in any financial transaction. such data includes, but not limited to, account numbers, authentication credentials, card numbers, card verification codes or values, and customer numbers;
  - consisting of unique identifiers issued by government agencies peculiar to an individual which includes, but not limited to, identification numbers, social security numbers, previous or current health records, and licenses; and
  - specifically established by law, regulation or executive order to be classified or confidential, including those that constitute "privileged communication."

- Outlines the scope of the DPA with qualified application on the processing of the following specific information:
  - information necessary in order to carry out the functions of public authorities, for information sharing necessary for the investigation and prosecution of child pornography and other forms of child exploitation, terrorism, and trafficking in persons;
  - information by courts acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks; and
  - information necessary for the audit functions and to safeguard the independence of the Commission on Audit (COA) in the performance of its constitutional mandate, as well as those information necessary for departments, bureaus, offices, agencies, and instrumentalities of the national government, LGUs, GOCCs, and all other entities, including private entities affected by or under the jurisdiction of the COA.

- Redefines the extraterritorial application of the DPA that the processing of personal information relates to a Philippine citizen or resident who are in the Philippines, where the processing activities of a natural or juridical person outside the Philippines involve offering of goods or services or monitoring of behavior within the Philippines.

- Explains the criteria under section 12 of the DPA for lawful processing of personal information when the data subject has given his or her consent. In specific case of information society providers offering services directly to a child, the processing of the personal information of a child shall be lawful where the child is more than 15 years old. Where the child is 15 years old or below, such
processing shall be lawful only if and to the extent that consent is given or authorized by persons exercising parental authority over the child.

- Explains the criteria under Section 13 of the DPA for Lawful processing of sensitive personal information, to wit:
  
  o the processing of information is pursuant to a contract freely entered into by the data subject and personal information controller;
  
  o the processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body with a charitable, religious, professional or similar purpose, in the course of its legitimate activities and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the personal information are not disclosed outside that body without the consent of the data subjects;
  
  o the processing is necessary for the purpose of medical diagnosis and treatment, preventive or occupational medicine, and the management and quality assurance of health or social care systems and services, and is carried out by a health care institution, health care provider, or a person under their responsibility bound by a professional or legal obligation of confidentiality; and
  
  o the processing is necessary for reasons of public interest in the area of public health or humanitarian emergencies.

- Clarifies the functions of the NPC, to wit:
  
  o primary jurisdiction over cases involving violations of the DPA;
  
  o issue summons, subpoena and subpoena duces tecum;
  
  o to hold and punish for contempt those who disregard orders or writs;
  
  o impose administrative sanctions, including monetary penalties for the violation of the DPA, its IRR, and NPC issuances or for failure or refusal to comply with compliance orders/resolutions; and
  
  o conduct seminars, conferences and trainings for awareness and capacity building relative to its mandate.

- Provides for administrative sanctions and the use of fines and fees, to wit:
  
  o Administrative fines not to exceed five (5) million pesos per violation.
  
  o Impose sanctions, including administrative fines, warning or reprimand for violation of the DPA, its IRR, or for failure or refusal to comply with NPC orders/resolutions/other issuances.
  
  o Imposition of the administrative sanctions or award of civil indemnity – without prejudice to the filing of criminal charges.
  
  o Authorized to retain, subject only to the existing accounting and auditing rules and regulations, all the fees, fines, royalties and other charges, collected by the Commission, for use in its operations, to improve the delivery of its services to the public.
- Provides for penal provisions which indicate “OR” between imprisonment and fine and added an option “OR BOTH” at the end of provision so that the decision on which penalty to be imposed shall be left to the discretion of the proper court.

- Removes “consent of the data subject” and modified it to refer to “lawful basis for processing” or “authority under the Act or existing law”.

- Provides that if the offender is a public official or employee, in addition to the penalties prescribed under the Act, shall suffer perpetual or temporary absolute disqualification from office.

RELATED LAWS:

- Republic Act No. 10173  (The Data Privacy Act of 2012)
- Republic Act No. 386  (The New Civil Code of the Philippines)
- Presidential Decree (The Government Auditing Code of the Philippines)
- Republic Act No. 9160, as amended, (The Anti-Money Laundering Act)
- Republic Act No. 9510, (The Credit Information System Act)
- Republic Act No. 1405, (The Secrecy of Bank Deposits Act)
- Republic Act No. 6426, (The Foreign Currency Deposit Act)