



HOUSE OF REPRESENTATIVES

House Bill No. 5612

Introduced by Representative VICTOR A. YAP

EXPLANATORY NOTE

In 1968, the Supreme Court declared that “The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection.”¹ Today, more than 50 years later, one aspect of this right, that of informational privacy, insists on the same recognition. Information coupled with advancements in technology brought in the age of big data, artificial intelligence, and the internet of things—a critical component of which is the processing of personal information. The challenge for us is how to maximize the benefits of the 4th industrial revolution while ensuring the protection of individuals from exploitation and misuse of their personal information.

Republic Act No. 10173 or the Data Privacy Act was promulgated in 2012 with the intent of protecting individual personal information by imposing obligations on all those who collect and process personal information, whether in the government or the private sector. This law was influenced by the EU’s Directive 95/46/EC (1995 Directive) and the APEC privacy principles. Since then, we have been facing new challenges and threats to privacy vis-à-vis the digital transformation and utilization of innovative information and communication technologies.

As a response to these changes, the European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016, which took effect in 2018, repealing the Directive which influenced our own DPA. Likewise, the Council of Europe modernized its Convention 108 in 2018, the only international legally binding instrument on the protection of private life and personal data which is open for accession to any country in the world. Many APEC Economies and ASEAN countries have undergone or are undergoing legal reforms for data protection, among them Japan, California, Malaysia, and Thailand.

The Philippines is an emerging leader in data protection, with the Philippine’s National Privacy Commission elected to the Executive Committee of the International Conference of Data Protection and Privacy Commissioners, the premier global forum for data protection authorities for nearly four decades. A strong data protection regime is not only necessary to protect the rights of Filipino data subjects, but it is at the same time a critical component of national development, from building people’s trust in government to generating revenues for the Philippine economy. Trust in the banking industry and financial technology, or in the business process outsourcing sector, or in the e-health initiatives mean innovation and growth, and this trust depends on ensuring the resilience of personal data processing systems.

¹Morfe v. Mutuc, 22 SCRA 424 (1968)

In order to strengthen the implementation of the Data Privacy Act, and align our law with international standards, there is a need to introduce amendments to the Data Privacy Act. This bill takes into consideration the strengths of the current law and areas for improvement in order to respond to the changing times.

Among the amendments introduced in this bill are provisions that will address concerns on child online protection, by requiring parental consent for online services offered directly to children 15 years old or below.² The bill also clarifies the definition of what constitutes sensitive personal information and the requirements for personal data breach notification. This aligns the criteria for lawful processing of personal information with international standards, allowing processing for public health purpose and humanitarian emergencies, among others.

This bill will strengthen the implementation of the Data Privacy Act by declaring definitive functions of the National Privacy Commission in the exercise of its quasi-judicial powers and in the effective enforcement of its orders. In the past years, the Commission has been receiving concerns and complaints from data subjects, with more than one thousand complaints being filed in the first half of 2019 alone.

Considering government initiatives that will involve processing of personal data, business models capitalizing on use of personal information, and emerging threats to data protection, the need to cultivate a culture of privacy and to strengthen the Data Privacy Act is urgently needed. This bill will 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.

For the foregoing reasons, early approval of this bill is earnestly sought.



REP. VICTOR A. YAP
Second District, Province of Tarlac

²GDPR age is 16, but 15 years of age was recommended since this aligned with Juvenile Justice Law

HOUSE OF REPRESENTATIVES

House Bill No. 5612

Introduced by Representative VICTOR A. YAP

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

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

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) *Data subject* refers to [an individual] A NATURAL PERSON whose personal information is
processed.

[(d) Direct marketing refers to communication by whatever means of any advertising or
marketing material which is directed to particular individuals.]

[(e)] (D) *Filing system* refers to any act 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)] (E) *Information and Communications System* refers to a system for generating, sending,
receiving, storing or otherwise processing electronic data messages or electronic documents
and includes the computer system or other similar device by or 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.

[(g)] (F) *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.

(G) PERSONAL DATA BREACH MEANS 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.

(h) *Personal information controller* refers to a NATURAL OR JURIDICAL person, PUBLIC
AUTHORITY, AGENCY OR OTHER ENTITY WHICH, ALONE OR JOINTLY WITH

OTHERS, or organization who [controls the collection, holding,] DETERMINES THE PURPOSES AND MEANS OF THE processing [or use] of personal information, including a person or organization who instructs another person or organization to [collect, hold,] process, [use, transfer or disclose] personal information on his or her behalf. The term excludes:

xxx

(i) *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) *Processing* refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, 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) *Sensitive personal information* refers to personal information:

(1) About an individual's [race] RACIAL or ethnic origin, [marital status, age, color, and] religious, philosophical BELIEF, LABOR or political affiliations;

(2) About an individual's health, [education,] genetic DATA, BIOMETRIC DATA, [or]sexual life, SEXUAL ORIENTATION OR GENDER IDENTITY, 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) ABOUT AN INDIVIDUAL'S FINANCIAL DATA;

[(3)] (4) Issued by government agencies peculiar to an individual which includes, but not limited to, IDENTIFICATION NUMBERS, social security numbers, previous or current health records, licenses [or its denials, suspension or revocation], and tax returns;

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

SECTION 2. Section 4 of the same Act is hereby amended as follows:

"SEC. 4. *Scope*. The Act shall apply to the processing of all types of personal information AND COMMUNICATION SYSTEMS OR ANY FILING SYSTEM BY[and to] any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately preceding paragraph: Provided, That the requirements of Section 5 are complied within THE GOVERNMENT OR PRIVATE SECTOR, SUBJECT TO THE PROVISIONS ON EXTRATERRITORIAL APPLICATION.

This Act does not apply to the following:

(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 HIS OR HER POSITION OR functions [of the individual], 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, SUCH AS THE GRANTING OF A LICENSE OR PERMIT, 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) Processing of information for journalistic, artistic, OR literary purpose, [or research purposes] IN ORDER TO UPHOLD FREEDOM OF SPEECH, OF EXPRESSION, OR OF 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; [and

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

1 (F) PROCESSING OF INFORMATION NECESSARY IN ORDER TO CARRY OUT THE
2 FUNCTIONS OF LAW ENFORCEMENT OR REGULATORY AUTHORITIES, INCLUDING
3 THE PERFORMANCE OF THE FUNCTIONS OF THE INDEPENDENT, CENTRAL
4 MONETARY AUTHORITY AND INFORMATION SHARING NECESSARY FOR THE
5 INVESTIGATION AND PROSECUTION OF CHILD PORNOGRAPHY AND OTHER
6 FORMS OF CHILD EXPLOITATION, IN ACCORDANCE WITH THEIR
7 CONSTITUTIONALLY OR STATUTORILY MANDATED FUNCTION: PROVIDED, THAT
8 PROTECTION OF FUNDAMENTAL FREEDOMS ARE GUARANTEED;

9
10 (G) PROCESSING OF INFORMATION BY COURTS ACTING IN THEIR JUDICIAL
11 CAPACITY, IN ORDER TO SAFEGUARD THE INDEPENDENCE OF THE JUDICIARY IN
12 THE PERFORMANCE OF ITS JUDICIAL TASKS; AND

13
14 (H) PROCESSING OF INFORMATION BY A NATURAL PERSON FOR PURPOSE OF A
15 PURELY PERSONAL OR HOUSEHOLD ACTIVITY;

16
17 PROVIDED, THAT THE REASONABLE FREEDOM GRANTED BY THIS ACT DO NOT
18 EXTEND TO PERSONAL INFORMATION CONTROLLERS OR PERSONAL
19 INFORMATION PROCESSORS, WHO REMAIN SUBJECT TO THE REQUIREMENTS OF
20 IMPLEMENTING SECURITY MEASURES FOR PERSONAL DATA PROTECTION:
21 PROVIDED FURTHER, THAT THE PROCESSING OF THE INFORMATION PROVIDED IN
22 THE PRECEDING PARAGRAPHS SHALL BE EXEMPTED FROM THE REQUIREMENTS OF
23 THE ACT ONLY TO THE MINIMUM EXTENT NECESSARY TO ACHIEVE THE SPECIFIC
24 PURPOSE, FUNCTION, OR ACTIVITY.”

25
26 SECTION 3. Section 6 of the same Act is hereby amended as follows:

27
28 “SEC. 6. Extraterritorial Application. – This Act applies to an act done or practice engaged in
29 and outside of the Philippines by an entity if:

30
31 [(a) The act, practice or processing relates to personal information about a Philippine
32 citizen or a resident;

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

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

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

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

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

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

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

44
45 (A) THE NATURAL OR JURIDICAL PERSON INVOLVED IN THE PROCESSING OF
46 PERSONAL INFORMATION IS FOUND OR ESTABLISHED IN THE PHILIPPINES;

47
48 (B) THE PROCESSING OF PERSONAL INFORMATION IS BEING DONE IN THE
49 PHILIPPINES;

50
51 (C) THE PROCESSING OF PERSONAL INFORMATION RELATES TO A PHILIPPINE
52 CITIZEN OR RESIDENT WHO ARE IN THE PHILIPPINES, WHERE THE
53 PROCESSING ACTIVITIES OF A NATURAL OR JURIDICAL PERSON OUTSIDE
54 THE PHILIPPINES INVOLVES OFFERING OF GOODS OR SERVICES, OR
55 MONITORING OF BEHAVIOR WITHIN THE PHILIPPINES; OR

(D) THE PROCESSING RELATES TO PERSONAL INFORMATION OF A PHILIPPINE CITIZEN OR A RESIDENT, AND THE ENTITY HAS A LINK WITH THE PHILIPPINES. THIS INCLUDES:

1. USE OF EQUIPMENT LOCATED IN THE COUNTRY, OR MAINTAINS AN OFFICE, BRANCH OR AGENCY IN THE PHILIPPINES FOR PROCESSING OF PERSONAL INFORMATION.
2. A CONTRACT IS ENTERED IN THE PHILIPPINES;
3. A JURIDICAL ENTITY UNINCORPORATED IN THE PHILIPPINES BUT HAS CENTRAL MANAGEMENT AND CONTROL IN THE COUNTRY;
4. 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;
5. AN ENTITY THAT CARRIES ON BUSINESS IN THE PHILIPPINES;
6. AN ENTITY THAT COLLECTS OR HOLDS PERSONAL INFORMATION IN THE PHILIPPINES."

SECTION 4. Section 7 of the same Act is hereby amended 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 ALLEGED VIOLATORS OR WITNESSES 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 THE VIOLATION OF 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

1 NUMBER OF AFFECTED DATA SUBJECTS; PROVIDED, FURTHER: THAT SUCH
2 ADMINISTRATIVE FINES SHALL NOT BE MORE THAN FIVE MILLION PESOS
3 (P5,000,000) PER VIOLATION;
4

5 [(d)] (F) Compel or petition any entity, government agency or instrumentality to abide by
6 its orders or take action on a matter affecting data privacy, OR TO PROVIDE
7 ASSISTANCE FOR THE EFFECTIVE IMPLEMENTATION OF THE ACT;
8

9 [(e)] (G) Monitor the compliance [of other government agencies or
10 instrumentalities]PERSONAL INFORMATION CONTROLLERS AND PERSONAL
11 INFORMATION PROCESSORS on their security and technical measures and recommend
12 the necessary action in order to meet minimum standards for the protection of personal
13 information pursuant to this Act;
14

15 [(f)] (H) Coordinate with other government agencies and the private sector on efforts to
16 formulate and implement plans and policies to strengthen the protection of personal
17 information in the country;
18

19 (I) CONDUCT SEMINARS, CONFERENCES AND TRAININGS FOR AWARENESS AND
20 CAPACITY BUILDING IN RELATION TO ITS MANDATE, AND FOR THIS PURPOSE
21 MAY COLLECT REASONABLE FEES FROM GOVERNMENT AND PRIVATE AGENCY
22 PARTICIPANTS BASED ON PRESCRIBED RATES IN RELEVANT LAW AND
23 REGULATIONS: PROVIDED, THAT PROCEEDS COLLECTED MAY BE USED FOR THE
24 CONTINUING CONDUCT OF SUCH SEMINARS, CONFERENCES, AND TRAININGS
25 SUBJECT TO BUDGETING, ACCOUNTING AND AUDITING RULES AND
26 REGULATIONS;
27

28 [(g)] (J) Publish on a regular basis a guide to all laws relating to data protection, AND
29 PREPARE REPORTS ON DISPOSITION OF COMPLAINTS AND RESOLUTION OF ANY
30 INVESTIGATION IT INITIATES, AND, IN CASES IT DEEMS APPROPRIATE,
31 PUBLICIZE ANY SUCH REPORT;

32 [(h)] (K) Publish a compilation of agency system of records and notices, including index
33 and other finding aids;

34 [(i)] (L) Recommend to the Department of Justice (DOJ) the prosecution and imposition of
35 penalties specified in [Sections 25 to 29 of] this Act;

36 [(j)] (M) Review, approve, reject or require modification of privacy codes voluntarily
37 adhered to by personal information controllers: Provided, That the privacy codes shall
38 adhere to the underlying data privacy principles embodied in this Act: Provided, further,
39 That such privacy codes may include private dispute resolution mechanisms for
40 complaints against any participating personal information controller. For this purpose, the
41 Commission shall consult with relevant regulatory agencies in the formulation and
42 administration of privacy codes applying the standards set out in this Act, with respect to
43 the persons, entities, business activities and business sectors that said regulatory bodies are
44 authorized to principally regulate pursuant to the law: Provided, finally. That the
45 Commission may review such privacy codes and require changes thereto for purposes of
46 complying with this Act;

47 [(k)] (N) Provide assistance on matters relating to privacy or data protection at the request
48 of a national or local agency, a private entity or any person;

49 [(l)] (O) Comment on the implication on data privacy of proposed national or local statutes,
50 regulations or procedures, issue advisory opinions and interpret the provisions of this Act
51 and other data privacy laws;

1 [(m)] (P) Propose legislation, amendments or modifications to Philippine laws on privacy
2 or data protection as may be necessary;

3 [(n)] (Q) Ensure proper and effective coordination with data privacy regulators in other
4 countries and private accountability agents, participate in international and regional
5 initiatives for data privacy protection;

6 [(o)] (R) Negotiate and contract with other data privacy authorities of other countries for
7 cross-border application and implementation of respective privacy laws;

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

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

13
14 SECTION 5. Section 9 of the same Act is hereby amended as follows:

15
16 “SEC. 9. *Organizational Structure of the Commission.* – The Commission shall be attached to
17 the Department of Information and Communications Technology (DICT) and shall be
18 headed by a Privacy Commissioner, who shall also act as Chairman of the Commission.
19 The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners,
20 one to be responsible for [Data Processing Systems] COMPLIANCE MONITORING and
21 one to be responsible for [Policies and Planning] POLICY AND STANDARDS. The Privacy
22 Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the
23 President of the Philippines for a term of [three (3)] FOUR (4) years, and may be
24 reappointed for another term of [three (3)] FOUR (4) years. Vacancies in the Commission
25 shall be filled in the same manner in which the original appointment was made:
26 PROVIDED, THAT IN CASE OF EXPIRATION OF TERM AND NO COMMISSIONER OR
27 DEPUTY PRIVACY COMMISSIONER IS APPOINTED, THE COMMISSIONER OR
28 DEPUTY PRIVACY COMMISSIONER, AS THE CASE MAY BE, SHALL HOLD OFFICE
29 IN A HOLD-OVER CAPACITY UNTIL SUCH APPOINTMENT SHALL HAVE BEEN
30 DULY ISSUED: PROVIDED FURTHER, THAT IN CASE A VACANCY OCCURS BEFORE
31 THE EXPIRATION OF THE TERM OF OFFICE, THE APPOINTMENT TO SUCH
32 VACANCY SHALL ONLY BE FOR THE UNEXPIRED TERM OF THE PREDECESSOR.

33
34 Xxx”

35
36 SECTION 6. Section 11 of the same Act is hereby amended as follows:

37
38 “SEC.11. *General Data Privacy Principles.* The processing of personal information shall be
39 allowed, subject to compliance with the requirements of the Act and other laws allowing
40 disclosure of information to the public, and adherence to the principles of transparency,
41 legitimate purpose, and proportionality.

42
43 Personal information must be:

44
45 Xxx

46
47 (c) Accurate,[relevant,] and, where necessary for purposes for which it is to be used the
48 processing of personal information, kept up to date; inaccurate or incomplete data, having
49 regard to the purposes for which they are processed, must be rectified, supplemented,
50 destroyed or their further processing restricted;

51
52 (d) Adequate, RELEVANT and not excessive in relation to the purposes for which they are
53 collected and further processed;

1
2 Xxx
3

4 (f) Kept in a form which permits identification of data subjects for no longer than is
5 necessary for the purposes for which the data were collected and processed: Provided,
6 That personal information collected for other purposes may be processed OR STORED
7 LONGER SOLELY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, for
8 historical, statistical or scientific purposes, and in cases laid down in law may be stored for
9 longer periods [: Provided, further, That adequate safeguards are guaranteed by said laws
10 authorizing their processing], SUBJECT TO IMPLEMENTATION OF ADEQUATE
11 SAFEGUARDS FOR DATA PROTECTION.
12

13 (G) PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY OF THE
14 PERSONAL INFORMATION.
15

16 The personal information controller must ensure implementation of personal information
17 processing principles set out herein.”
18

19 SECTION 7. Section 12 of the same Act is hereby amended as follows:
20

21 “SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of
22 personal information shall be permitted only if not otherwise prohibited by law,
23 INCLUDING THE RESTRICTIONS IN THE PROCESSING OF SENSITIVE PERSONAL
24 INFORMATION, and when at least one of the following conditions exists:
25

26 (a) The data subject has given his or her consent: PROVIDED, THAT IN THE SPECIFIC
27 CASE OF AN INFORMATION SOCIETY PROVIDERS OFFERING SERVICES DIRECTLY
28 TO A CHILD, THE PROCESSING OF THE PERSONAL INFORMATION OF A CHILD
29 SHALL BE LAWFUL WHERE THE CHILD IS MORE THAN 15 YEARS OLD. WHERE THE
30 CHILD IS 15 YEARS OLD OR BELOW, SUCH PROCESSING SHALL BE LAWFUL ONLY IF
31 AND TO THE EXTENT THAT CONSENT IS GIVEN OR AUTHORIZED BY PERSONS
32 EXERCISING PARENTAL AUTHORITY OVER THE CHILD;
33

34 (b) The processing [of personal information] is necessary and is related to the fulfillment of
35 a contract with the data subject or in order to take steps at the request of the data subject
36 prior to entering into a contract;
37

38 Xxx
39

40 (d) The processing is necessary to protect vitally important interests of the data subject or OF
41 ANOTHER NATURAL PERSON, including life and health;
42

43 Xxx”
44

45 SECTION 8. Section 13 of the same Act is hereby amended as follows:
46

47 “SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive
48 personal information and privileged information shall be prohibited, except in the following
49 cases:
50

51 (a) The data subject has given his or her consent, specific to the purpose prior to the
52 processing, or in the case of privileged information, all parties to the exchange have
53 given their consent prior to processing, EXCEPT IF A SPECIFIC LAW PROVIDES THAT
54 THE PROHIBITION FROM PROCESSING MAY NOT BE LIFTED BY THE DATA
55 SUBJECT;
56

1 (B) THE PROCESSING OF INFORMATION IS PURSUANT TO A CONTRACT FREELY
2 ENTERED INTO BY THE DATA SUBJECT AND PERSONAL INFORMATION
3 CONTROLLER: *PROVIDED*, THAT THE PERFORMANCE OF THE CONTRACT OR
4 PROVISION OF THE SERVICE IS NOT MADE CONDITIONAL ON CONSENTING TO
5 THE PROCESSING OF SENSITIVE PERSONAL INFORMATION THAT IS NOT
6 NECESSARY TO THE OBJECT OF THE CONTRACT;
7

8 [(b)] (C) The processing of the same is provided for by existing laws and
9 regulations: *Provided*, That such regulatory enactments OR ITS IMPLEMENTING RULES
10 guarantee the protection of the sensitive personal information and the privileged
11 information: *Provided, further*, That the consent of the data subjects are not required by law or
12 regulation permitting the processing of the sensitive personal information;
13

14 [(c)] (D) The processing is necessary to protect the life and health of the data subject or
15 another person, and the data subject is not legally or physically able to express his or her
16 consent prior to the processing;
17

18 [(d)] The processing is necessary to achieve the lawful and non-commercial objectives of
19 public organizations and their associations: *Provided*, That such processing is only confined
20 and related to the bona fide members of these organizations or their associations: *Provided*,
21 further, That the sensitive personal information are not transferred to third parties: *Provided*,
22 finally, That consent of the data subject was obtained prior to processing;
23

24 (E) THE PROCESSING IS CARRIED OUT WITH APPROPRIATE SAFEGUARDS BY A
25 FOUNDATION, ASSOCIATION OR ANY OTHER NOT-FOR-PROFIT BODY WITH A
26 CHARITABLE, RELIGIOUS, PROFESSIONAL OR SIMILAR PURPOSE, IN THE COURSE
27 OF ITS LEGITIMATE ACTIVITIES AND ON CONDITION THAT THE PROCESSING
28 RELATES SOLELY TO THE MEMBERS OR TO FORMER MEMBERS OF THE BODY OR TO
29 PERSONS WHO HAVE REGULAR CONTACT WITH IT IN CONNECTION WITH ITS
30 PURPOSES, AND THAT THE PERSONAL INFORMATION ARE NOT DISCLOSED
31 OUTSIDE THAT BODY WITHOUT THE CONSENT OF THE DATA SUBJECTS;
32

33 (F) THE PROCESSING RELATES TO INFORMATION WHICH ARE MANIFESTLY MADE
34 PUBLIC BY THE DATA SUBJECT: *PROVIDED* THAT FURTHER PROCESSING SHALL
35 NOT BE CONTRARY TO LAW, MORALS, GOOD CUSTOMS, PUBLIC ORDER OR PUBLIC
36 POLICY;
37

38 [(E)] (G) The processing is necessary for the purpose of medical DIAGNOSIS AND
39 treatment, PREVENTIVE OR OCCUPATIONAL MEDICINE, AND THE MANAGEMENT
40 AND QUALITY ASSURANCE OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES,
41 AND is carried out by a [medical practitioner or a medical treatment] HEALTH CARE
42 institution, [and an adequate level of protection of personal information is
43 ensured] HEALTH CARE PROVIDER, OR A PERSON UNDER THEIR RESPONSIBILITY
44 BOUND BY A PROFESSIONAL OR LEGAL OBLIGATION OF CONFIDENTIALITY,
45 *PROVIDED*: THAT ADEQUATE SECURITY MEASURES ARE IMPLEMENTED FOR THE
46 PROTECTION OF SENSITIVE PERSONAL INFORMATION;
47

48 (H) THE PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE
49 AREA OF PUBLIC HEALTH OR HUMANITARIAN EMERGENCIES, *PROVIDED*: THAT
50 SUCH PROCESSING IS COVERED BY REGULATORY ENACTMENTS ENSURING
51 NECESSITY OF PROCESSING AND IMPLEMENTATION OF
52 APPROPRIATE SAFEGUARDS FOR DATA PROTECTION;
53

54 [(f)] (I) The processing [concerns such personal information as] is necessary for the
55 protection of lawful rights and interests of natural or legal persons in court proceedings, or
56 the establishment, exercise or defense of legal claims, or [when provided to government or
57 public authority] WHENEVER COURTS ARE ACTING IN THEIR JUDICIAL CAPACITY;

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

(K) THE PROCESSING PERTAINS TO INFORMATION ORIGINALLY COLLECTED FROM RESIDENTS OF FOREIGN JURISDICTIONS BEING PROCESSED IN THE PHILIPPINES: PROVIDED, THAT THE COLLECTION IS IN ACCORDANCE WITH THE LAWS OF THOSE FOREIGN JURISDICTIONS, INCLUDING ANY APPLICABLE DATA PRIVACY LAWS;

SECTION 9. Section 16 of the same Act is hereby amended 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 SHOULD 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 MUST be [furnished] PROVIDED the information indicated hereunder 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;
- [(2)] (3) Purposes [for which they are being or are to be processed] and Lawful basis of processing;
- [(3)] (4) Scope and method of the personal information processing;
- (5) Sources of personal information, and where applicable, whether it came from publicly accessible sources;
- [(4)] (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 PERIOD; and
- [(8)] (11) The existence of their rights as DATA SUBJECTS, to access, correction, 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 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 be informed of its inaccuracy and its rectification upon reasonable request of the data subject;

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

(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 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, ON GROUNDS RELATING TO HIS OR HER PARTICULAR SITUATION, AT ANY TIME TO PROCESSING OF PERSONAL INFORMATION CONCERNING HIM OR HER. 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 CONTROLLER SHALL NO LONGER PROCESS THE PERSONAL INFORMATION UNLESS THE CONTROLLER DEMONSTRATES COMPELLING LEGITIMATE GROUNDS FOR THE 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 PARAGRAPH.

WHEN A DATA SUBJECT OBJECTS OR WITHHOLDS CONSENT, THE PERSONAL INFORMATION CONTROLLER SHALL NO LONGER PROCESS THE PERSONAL INFORMATION, UNLESS, OR THE PROCESSING IS NEEDED PURSUANT TO A SUBPOENA, OR THE PROCESSING IS REQUIRED BY RELEVANT LAW AND REGULATION.

(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 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;

TAKING INTO ACCOUNT THE PURPOSES OF THE PROCESSING, THE DATA SUBJECT SHALL HAVE THE RIGHT TO HAVE INCOMPLETE PERSONAL INFORMATION COMPLETED, 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 PERTAINING TO HIM OR HER FROM THE PERSONAL INFORMATION CONTROLLER'S FILING SYSTEM, WHERE:

- A) THE PERSONAL INFORMATION IS INCOMPLETE, OUTDATED, FALSE, OR UNLAWFULLY OBTAINED;
- B) THE PERSONAL INFORMATION IS BEING USED FOR PURPOSE NOT AUTHORIZED BY THE DATA SUBJECT;
- C) THE PERSONAL INFORMATION IS NO LONGER NECESSARY FOR THE PURPOSES FOR WHICH THEY WERE COLLECTED;
- D) THE DATA SUBJECT WITHDRAWS CONSENT OR OBJECTS TO THE PROCESSING, AND THERE IS NO OTHER LEGAL GROUND OR OVERRIDING LEGITIMATE INTEREST FOR THE PROCESSING;
- E) THE PERSONAL INFORMATION CONCERNS PRIVATE INFORMATION THAT IS PREJUDICIAL TO DATA SUBJECT, UNLESS JUSTIFIED BY FREEDOM OF SPEECH, OF EXPRESSION, OR OF THE PRESS OR OTHERWISE AUTHORIZED;
- F) THE PROCESSING IS UNLAWFUL; OR
- G) 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.

(F) RIGHT TO CLAIM DAMAGES. THE DATA SUBJECT HAS THE RIGHT TO BE INDEMNIFIED FOR ANY DAMAGES 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 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 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

1 INFORMATION shall be used only for the declared purpose. [Likewise, the
2 immediately preceding sections are not applicable to the] THE LIMITATION ALSO
3 APPLIES WHEN SPECIFICALLY PROVIDED BY LAW, OR REGULATION, WHEN
4 NECESSARY TO PROTECT LIFE AND HEALTH OF DATA SUBJECTS, OR WHERE the
5 processing of personal information gathered for the purpose of investigations in relation
6 to any criminal, administrative or tax liabilities of a data subject.”
7

8 SECTION 11. Section 20 of the same Act is hereby amended as follows:
9

10 “SEC. 20. Security of Personal Information.
11

12 Xxx
13

14 (e) The personal information controller shall [promptly] notify the Commission and
15 affected data subjects [when sensitive personal information or other information that
16 may, under the circumstances, be used to enable identity fraud are reasonably
17 believed to have been acquired by an unauthorized person, and the personal
18 information controller or the Commission believes that such unauthorized acquisition
19 is likely to give rise to a real risk of serious harm to any affected data subject]
20 WITHIN 72 HOURS UPON BEING AWARE OR UPON REASONABLE BELIEF
21 THAT A PERSONAL DATA BREACH INVOLVING SENSITIVE PERSONAL
22 INFORMATION OR OTHER INFORMATION THAT MAY BE USED TO ENABLE
23 IDENTITY FRAUD OCCURRED. The notification shall at least describe the nature of
24 the breach, the [sensitive] personal information possibly involved, and the measures
25 taken by the entity to address the breach. [Notification may be delayed only to the
26 extent necessary to determine the scope of the breach, to prevent further disclosures,
27 or to restore reasonable integrity to the information and communications system.]
28 WHERE SUCH NOTIFICATION CANNOT BE ACHIEVED WITHIN 72 HOURS,
29 THE REASONS FOR THE DELAY SHOULD ACCOMPANY THE NOTIFICATION
30 AND INFORMATION MAY BE PROVIDED IN PHASES WITHOUT ANY FURTHER
31 DELAY.
32

33 [(1) In evaluating if notification is unwarranted, the Commission may take into
34 account compliance by the personal information controller with this section and
35 existence of good faith in the acquisition of personal information.]
36

37 [(2)] (1) The Commission may exempt a personal information controller from
38 notification OF DATA SUBJECT where, in its reasonable judgment, such notification
39 would not be in the public interest or in the interests of the affected data subjects. IN
40 EVALUATING IF NOTIFICATION IS UNWARRANTED, THE COMMISSION MAY
41 TAKE INTO ACCOUNT COMPLIANCE BY THE PERSONAL INFORMATION
42 CONTROLLER WITH THIS ACT AND EXISTING SECURITY MEASURES
43 SHOWING THAT THE PERSONAL DATA BREACH IS UNLIKELY TO RESULT IN
44 A RISK TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS.
45

46 [(3)] (2) The Commission may authorize postponement of notification where it may
47 hinder the progress of a criminal investigation related to a serious breach.
48 NOTIFICATION OF DATA SUBJECTS MAY BE DELAYED ONLY TO THE EXTENT
49 NECESSARY TO DETERMINE THE SCOPE OF THE BREACH, TO PREVENT
50 FURTHER DISCLOSURES, OR TO RESTORE REASONABLE INTEGRITY TO THE
51 INFORMATION AND COMMUNICATIONS SYSTEM. WHERE THE PERSONAL
52 DATA BREACH IS LIKELY TO RESULT IN A HIGH RISK TO THE RIGHTS AND
53 FREEDOMS OF THE NATURAL PERSON, THE CONTROLLER SHOULD
54 COMMUNICATE TO THE DATA SUBJECT A PERSONAL DATA BREACH,
55 WITHOUT UNDUE DELAY, IN ORDER TO ALLOW HIM OR HER TO TAKE THE
56 NECESSARY PRECAUTIONS.
57

1 FOR PURPOSES OF THIS SECTION, THE PERSONAL INFORMATION
2 CONTROLLER SHALL ENSURE THAT PERSONAL INFORMATION PROCESSORS
3 WILL PROMPTLY REPORT THE OCCURRENCE OF A PERSONAL DATA
4 BREACH TO ALLOW FOR NOTIFICATION OF THE COMMISSION AND DATA
5 SUBJECTS WITHIN THE PRESCRIBED PERIOD: PROVIDED, THAT WHERE THE
6 PERSONAL INFORMATION CONTROLLER IS OUTSIDE THE PHILIPPINES AND
7 IS UNABLE TO COMPLY WITH THE NOTIFICATION REQUIREMENTS, THE
8 PERSONAL INFORMATION PROCESSOR WHERE THE PERSONAL DATA
9 BREACH OCCURRED SHALL SUBMIT THE BREACH NOTIFICATION TO THE
10 COMMISSION.”

11
12 SECTION 12. Section 21 of the same Act is hereby amended as follows:
13

14 “SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible
15 for personal information under its control or custody, including information that have
16 been transferred to a third party for processing, whether domestically or internationally,
17 subject to cross-border arrangement and cooperation.
18

19 a) The personal information controller is accountable for complying with the
20 requirements of this Act and shall use contractual or other reasonable means to
21 provide a comparable level of protection while the information are being processed
22 by a third party.
23

24 b) The personal information controller shall designate A DATA PROTECTION
25 OFFICER or an individual or individuals who are accountable for the organization’s
26 compliance with this Act. The identity of the individual(s) so designated shall be
27 made known to any data subject upon request.”
28

29 SECTION 13. Section 24 of the same Act is hereby amended as follows:
30

31 “SEC. 24. *Applicability to Government Contractors.* ACCESS TO PERSONAL
32 INFORMATION BY INDEPENDENT CONTRACTORS, CONSULTANTS, OR SERVICE
33 PROVIDERS ENGAGED BY A GOVERNMENT AGENCY SHALL BE GOVERNED BY
34 STRICT PROCEDURES CONTAINED IN FORMAL CONTRACTS, WHICH
35 PROVISIONS MUST COMPLY WITH THE ACT. In entering into any contract that may
36 involve accessing or requiring sensitive personal information from one thousand (1,000)
37 or more individuals, an agency shall require a contractor and its employees to register
38 their personal information processing system with the Commission in accordance with
39 this Act and to comply with the other provisions of this Act including the immediately
40 preceding section, in the same manner as agencies and government employees comply
41 with such requirements.”
42

43 SECTION 14. Section 36 of the same Act is hereby amended as follows:
44

45 “SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person
46 responsible for the offense is a public officer, as defined in the Administrative Code of the
47 Philippines in the exercise of his or her duties, an accessory penalty consisting in the
48 disqualification to occupy public office for a term double the term of criminal penalty
49 imposed shall be applied.
50

51 LIKEWISE, THE PUBLIC OFFICER, REGARDLESS OF WHETHER OR NOT HE OR SHE
52 HOLDS OFFICE OR EMPLOYMENT IN CASUAL, TEMPORARY, HOLDOVER,
53 PERMANENT OR REGULAR CAPACITY COMMITTING THE OFFENCE WILL BE
54 SUBJECT TO ADMINISTRATIVE PENALTIES UNDER THE REPUBLIC ACT NO. 6713,
55 OTHERWISE KNOWN AS THE “CODE OF CONDUCT AND ETHICAL STANDARDS
56 FOR PUBLIC OFFICIALS AND EMPLOYEES.”
57

1 SECTION 15. Section 37 of the same Act is hereby amended as follows:

2 “SEC. 37. *Restitution AND ADMINISTRATIVE SANCTIONS.* – THE COMMISSION
3 SHALL PUBLISH AND REGULARLY UPDATE A SCHEDULE OF ADMINISTRATIVE
4 FINES AS MAY BE DETERMINED BY THE COMMISSION TO BE APPROPRIATE,
5 TAKING INTO CONSIDERATION THE ATTENDANT CIRCUMSTANCES, SUCH AS
6 THE NATURE AND GRAVITY OF THE VIOLATION, AND NUMBER OF AFFECTED
7 DATA SUBJECTS, WHICH SHALL NOT EXCEED FIVE MILLION PESOS
8 (PHP5,000,000.00) PER VIOLATION.

9 AFTER DUE NOTICE AND HEARING, THE COMMISSION SHALL IMPOSE
10 SANCTIONS, INCLUDING ADMINISTRATIVE FINES, WARNING OR REPRIMAND,
11 UPON ANY PERSON FOR THE VIOLATION OF THIS ACT, ITS IMPLEMENTING
12 RULES AND REGULATIONS, OR FOR FAILURE OR REFUSAL TO COMPLY WITH
13 NPC ORDERS, RESOLUTIONS AND OTHER ISSUANCES.

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

17 THE IMPOSITION OF THE ADMINISTRATIVE SANCTIONS OR AWARD OF CIVIL
18 INDEMNITY SHALL BE WITHOUT PREJUDICE TO THE FILING OF CRIMINAL
19 CHARGES AGAINST THE PERSONS RESPONSIBLE FOR THE VIOLATION.”
20

21 SECTION 16. A new Section 41-A shall be inserted to read as follows:

22
23 “SEC. 41-A. *USE OF ADMINISTRATIVE FINES AND FEES.* FOR A MORE EFFECTIVE
24 AND EXPEDITIOUS IMPLEMENTATION OF THIS ACT, THE COMMISSION SHALL
25 BE AUTHORIZED TO RETAIN, WITHOUT NEED OF A SEPARATE APPROVAL FROM
26 ANY GOVERNMENT AGENCY, SUBJECT ONLY TO THE EXISTING ACCOUNTING
27 AND AUDITING RULES AND REGULATIONS, ALL THE FEES, FINES, ROYALTIES
28 AND OTHER CHARGES, COLLECTED BY THE COMMISSION UNDER THIS ACT,
29 FOR USE IN ITS OPERATIONS, LIKE UPGRADING OF ITS FACILITIES, EQUIPMENT
30 OUTLAY, HUMAN RESOURCE DEVELOPMENT, AND THE ACQUISITION OF THE
31 APPROPRIATE OFFICE SPACE, AMONG OTHERS, TO IMPROVE THE DELIVERY OF
32 ITS SERVICES TO THE PUBLIC. THIS AMOUNT, WHICH SHALL BE IN ADDITION
33 TO THE ANNUAL BUDGET OF THE COMMISSION, SHALL BE DEPOSITED AND
34 MAINTAINED IN A SEPARATE ACCOUNT OR FUND, WHICH MAY BE USED OR
35 DISBURSED DIRECTLY BY THE COMMISSION.”
36

37 SECTION 17. *Separability Clause.* – If any provision or part hereof is held invalid or
38 unconstitutional, the remainder of the law or the provision not otherwise affected shall remain
39 valid and subsisting.
40

41 SECTION 18. *Repealing Clause.* – All other laws, decrees, executive orders, proclamations
42 and administrative regulations or parts thereof inconsistent herewith are hereby repealed or
43 modified accordingly.
44

45 SECTION 19. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication
46 in at least two (2) national newspapers of general circulation.
47

48 Approved,
49