Republic of the Philippines
NATIONAL PRIVACY COMMISSION
Metro Manila

Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012"

Pursuant to the mandate of the National Privacy Commission to administer and implement the provisions of the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection, the following rules and regulations are hereby promulgated to effectively implement the provisions of the Act:

Rule I. Preliminary Provisions

Section 1. Title. These rules and regulations shall be known as the Implementing Rules and Regulations of Republic Act No. 10173 known as the Data Privacy Act of 2012, or the "Rules."

Section 2. Policy. These rules and regulations further enforce the Data Privacy Act and adopts generally accepted international principles and standards for data protection, safeguarding the fundamental right of every individual to privacy while supporting the free flow of information for innovation, growth and national development. These rules and regulations recognize the vital role of information and communications technology in nation-building and enforce the State's inherent obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected.

Section 3. Definitions. Whenever used in these Rules, the following terms shall have the respective meanings hereafter set forth:

*security incident – an event or occurrence that affects or tends to affect data protection, or that may compromise the availability, integrity and confidentiality of personal data, including those incidents that would have resulted to a security breach if not for safeguards in place
*data sharing – the disclosure or transfer of personal data under custody of a natural or juridical person or other entity involved in the processing of personal data to a third party, excludes outsourcing or instructions to personal information processor
*data processing systems – the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing

*automatic processing systems – the use of information and communications system to perform operation or set of operations on personal data involving under a logical framework or automated instructions

a. Act refers to the Data Privacy Act.

b. Breach is a security incident that leads to unlawful or unauthorized processing of personal, sensitive or privileged information, or that otherwise compromises the availability, integrity or confidentiality of personal data processed under the control of a personal information controller.

c. Commission refers to the National Privacy Commission created by virtue of the Data Privacy Act.

d. Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

.

e. Data subject refers to an individual whose personal, sensitive personal or privileged information is processed.

f. Direct marketing refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

g. 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.

h. 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.

i. Personal data is the term used when referring to personal information, sensitive personal information and privileged information collectively.

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.

k. Personal information controller refers to a natural or juridical person or any other body who controls the processing of personal data or instructs another to process personal data on his or her behalf. The term excludes:
   1. A natural or juridical person or any other body who performs such functions as instructed by another; or
   2. A natural person who processes personal data in connection with his or her personal, family or household affairs.

   There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of processing.

.

l. Personal information processor refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.

m. Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be by by automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.

n. Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication. For purpose of these rules, privileged information that is not personal information or sensitive personal information shall not be included.

o. Sensitive personal information refers to personal information:
   1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
   2. About an individual's health, education, genetic or sexual life 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. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
   4. Specifically established by an executive order or an act of Congress to be kept classified.

Rule II. Scope of Application

Section 4. Scope. The Data Privacy Act and these Rules apply to the processing of personal, sensitive personal or privileged information, in the government or private sector, under any of the following conditions:

a. The natural or juridical person involved in the processing of personal data is found or established in the Philippines.
b. The act, practice or processing relates to personal data about a Philippine citizen or Philippine resident.
c. The processing of personal data is being done in the Philippines.
d. The act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines, with due consideration to international law and comity, which may include:
   1. Use of equipment located in the country, or maintains an office, branch or agency in the Philippines for processing of personal data;
   2. A Contract 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 data; or
5. An entity that carries on business in the Philippines
6. An entity collects and holds personal data in the Philippines

Provided further, that the information is not specifically excluded in the succeeding section.

Section 5. Non-applicability. The Data Privacy Act does not apply to specific categories of information, to the extent of allowable collection, access, use, disclosure or other processing, laid down in the succeeding paragraphs. The non-applicability does not extend to the personal information controllers or processors, which process the same or other personal data, in a manner or for a purpose that is not specifically provided in this section.

a. The Act and these Rules shall not be used to restrict access to information that fall within matters of public concern, and for this purpose shall not apply to:
    1. Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
        (a) The fact that the individual is or was an officer or employee of the government institution;
        (b) The title, business address and office telephone number of the individual;
        (c) The classification, salary range and responsibilities of the position held by the individual; and
        (d) The name of the individual on a document prepared by the individual in the course of employment with the government.

    2. Information about an individual who is or was performing service under contract for a government institution only in so far as it 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;

    3. Information relating to a benefit of a financial nature conferred on an individual upon the discretion of 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 benefits given in the course of an ordinary transaction or as a matter of right are not discretionary benefits under these Rules.

b. The Act and these Rules do not apply to personal information processed for journalistic, artistic or literary purpose. It shall be considered for journalistic, artistic or literary purpose if processing is undertaken with view to publication or exhibition, upholding freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations. Any natural or juridical person or other body who shall process the same personal information for any purpose other than journalistic, artistic or literary, shall be covered by the Act and these Rules.

c. The Act and these Rules do not apply to personal information that will be processed for research purpose, subject to relevant provisions in the law or issuances of the Commission. Research covered by the Act shall be supported to the extent that research purposes will be achieved without compromising privacy and security of personal data, and rights of data subjects.

d. The Act and these Rules do not apply to information necessary in order to carry out functions of public authority only to the extent of collection and further processing consistent with a constitutionally or statutorily mandated function pertaining to law enforcement, public health, taxation and other regulatory function, including the performance of the functions of the independent, central monetary authority. The public authority must process the information, mindful of the rights of the individual data subject to privacy and security, and subject to other restrictions provided by law. If processing is by a personal information processor, the responsibility of the public authority as personal information controller remains. 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).

e. The Act and these Rules do not apply to information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas, and other bodies authorized by law, 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. Banks and financial institutions involved in processing of personal

data shall be covered by the act and these Rules where the information collected and processed to comply with law will be subjected to processing for other purpose.

f. The Rules shall not apply to 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, with regard to its collection. The Act and these Rules shall apply to processing performed in the Philippines, taking into account the law of the foreign jurisdiction with regard to collection. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be that of the Philippines.

The Act and these Rules shall not apply to 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. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, including proof that the law of the foreign jurisdiction specifically applies to processing in the Philippines, the applicable law shall be presumed to be the Act and these Rules.
(being reviewed)

Section 6. Protection Afforded to Journalists and their Sources.

a. Publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation shall not be compelled to reveal the source of any news report or information appearing in said publication if it was related in any confidence to such publisher, editor, or reporter.
b. Publishers, editors and duly accredited reporters who are likewise personal information controllers or processors within the meaning of the law are still bound to follow the Data Privacy Act and related issuances with regard to the processing of personal data, upholding rights of their data subjects and maintaining compliance with other provisions that are not incompatible with the protection provided by Republic Act No. 53.

Section 7. Protection afforded to Data Subjects.

a. Unless directly incompatible or inconsistent with the preceding sections, the personal information controller or

processor shall use reasonable means to protect the privacy and security of personal data.

b. The burden of proving that the Data Privacy Act is not applicable to a particular information falls on those involved in the processing of personal data or the party claiming the non-applicability.
c. In all cases, the determination of the applicability of the Data Privacy Act shall be liberally interpreted in favor of the rights and interests of the data subject.

Rule III. National Privacy Commission

Section 8. Mandate. The National Privacy Commission is an independent body mandated to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection.

Section 9. Functions. The National Privacy Commission shall have the following functions:

a. Rule Making. The Commission shall promulgate, review or amend its rules and regulations, and publish or issue administrative issuances for the effective implementation of the Act. This includes:
    1. Issue guidelines on security measures for personal data protection, encryption, and off-site access in government, and on the electronic format and technical standards for data portability;
    2. Issue standards for organizational, physical and technical security measures for data protection taking into account current data privacy best practices and most appropriate standard recognized by the information and communications technology industry;
    3. Consult with relevant regulatory agencies in the formulation of privacy standards or requirements to implement the Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to law;
    4. Propose legislation, amendments or modifications to Philippine laws on privacy or data protection, as may be necessary.

b. Advisory. The Commission shall be the advisory body on matters affecting data privacy and security. This includes:

1. Comment or report 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;
2. Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers, which may include private dispute resolution mechanisms for complaints against any participating personal information controller.

c. Public Education. The Commission shall undertake necessary or appropriate efforts to inform and educate the public of data privacy, data protection and fair information rights and responsibilities. This includes:
   1. Publish on a regular basis a guide to all laws relating to data protection;
   2. Publish a compilation of agency system of records and notices, including index and other finding aids;
   3. Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal data in the country;
   4. Document and report on the activities of the Commission in carrying out the provisions of the Act.

d. Compliance and Monitoring. The Commission shall perform compliance and monitoring functions to ensure effective implementation of the Act, these Rules and other issuances. This includes:
   1. Ensure compliance of personal information controllers with the provisions of the Act, including registration of data processing systems in the country, and notification prior to processing of personal data that could adversely affect the rights and freedoms of data subjects.
   2. Monitor the compliance of all government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal data pursuant to the Act;
   3. 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;
   4. Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws and generally

perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection;
5. Provide assistance on matters relating data protection at the request of a national or local agency, a private entity or any person, including enforcement of rights of data subject;
6. Assist Philippine companies doing business abroad to respond to data protection laws and regulations;
7. Manage the registration of the personal information processing system of contractors and its employees entering into contracts with government that involves accessing or requiring sensitive personal information from one thousand (1,000) or more individuals.

e. Complaints and Investigations. The Commission shall adjudicate on complaints and investigations arising from a privacy complaint, security breach, a violation of the rights of data subjects, and failure to comply with the Act, these rules and other issuances of the Commission. This includes:
   1. Receive complaints and institute investigations regarding a violation of the Act or the rights of data subjects, including reports of a Security Breach;
      For this purpose, the Commission may compel access to personal data that is subject of any complaint and to collect the information necessary to perform its functions under the Act, including the issuance of subpoena to compel testimony or production of evidence. In resolving any complaint or investigation, except where amicable settlement is reached by the parties, the Commission shall act as a collegial body.
   2. Facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, and adjudicate on matters affecting any personal data;
   3. Prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report.

f. Enforcement. The Commission shall do all acts as may be necessary to effectively implement the Data Privacy Act, these Rules and other issuances of the Commission, and to enforce its Orders, Resolutions or Decisions, including the imposition of sanctions, fines or penalties. This includes:
   1. Adjudicate privacy or security complaints and related issues and issue compliance or enforcement orders;
   2. Award indemnity on matters affecting privacy or security of personal data, or rights of data subjects;

3. Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal data, upon finding that the processing will be detrimental to national security, public interest, or in order to preserve and protect the rights of data subjects;
4. Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in the Act;
5. Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;
6. Impose fines and other administrative penalties for violations of the Act, these Rules, and other issuances of the Commission.

g. Other functions. The Commission shall exercise such other functions as may be necessary to fulfill its mandate under the law.

Section 10. Administrative Issuances. The Commission shall publish or issue official directives and administrative issuances, orders and circulars:

a. To govern the rules of procedure in the exercise of its quasi-judicial functions, subject to suppletory application of the Rules of Court;
b. To publish the schedule of fines and penalties for the violation of the Act, these Rules, issuances or the orders of the Commission and the fees for its administrative services and filing fees;
c. To provide or update the minimum standards for data protection, in addition to those already provided in these Rules, considering best practices or to account for the current state of information and communications technology and the generally accepted data privacy and security standards;
d. To give an advisory or legal opinions on matters affecting privacy and security of personal data;
e. To resolve a complaint or investigation and enforce its orders;
f. Other administrative issuances consistent with its mandate.

Section 11. Reports and Public Information. The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

Section 12. Confidentiality of Personal Data. The Commission shall ensure at all times the confidentiality of any personal data that comes to its knowledge and possession. Members, employees and consultants of the Commission, even after their term, employment or contract has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they were given access.

Section 13. Organizational Structure. The National Privacy Commission is attached to the Department of Information and Communications Technology for policy and program coordination in accordance with Section 38(3) of Executive Order No. 292 series of 1987. The Commission shall remain completely independent in the performance of its functions.

The Commission shall be headed by a Privacy Commissioner, who shall act as Chairman of the Commission. The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary.

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 Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

Section 14. Secretariat. The Commission is authorized to establish a Secretariat, which shall assist the Office of the Commissioner in the performance of its functions. The Secretariat shall be headed by an Executive Director and shall be organized according to the following offices:

a. Data Security and Compliance Office;
b. Legal and Enforcement Office;
c. Finance and Administrative Office;
d. Privacy Policy Office.

Majority of the members of the Secretariat, in so far as practicable, must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance

System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

The organizational structure shall be subject to review and modification of the Commission, including the creation of new divisions and units as it may deem necessary, and shall appoint officers and employees of the Commission in accordance with the civil service law, rules and regulations.

Section 15. Effect of Lawful Performance of Duty. The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: Provided, That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

Section 16. Magna Carta for Science and Technology Personnel. Qualified employees of the Commission shall be covered by Republic Act No. 8349, which provides a magna carta for scientists, engineers, researchers and other science and technology personnel in the government.

Rule IV. Data Privacy Principles

Section 17. General Principles. The processing of personal data shall be allowed, subject to compliance with the requirements of the Data Privacy Act, other laws allowing disclosure of information to the public and these Rules. All natural and juridical persons and other body involved in processing of personal data must ensure implementation of personal data processing principles set out in the Act, these Rules and other issuances of the Commission.

Section 18. Principles of Transparency, Legitimate Purpose and Proportionality. The processing of personal data shall adhere to the principles of transparency, legitimate purpose and proportionality.

a. Transparency. Processing of personal data shall be known to the data subject, who must be informed about the nature, purpose, method, and extent of processing; the rights of data

subject and how these can be exercised; and the identity and contact details of the personal information controller.

b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals or public policy.
c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose.

Section 19. General principles in collection, processing and retention. The processing of personal data shall adhere to the following general principles with regard to collection, processing and retention.

a. Collection must be for a specified and legitimate purpose
    1. There must be consent, which is time-bound, and may be withdrawn, unless specifically provided by Act or these Rules that consent for collection and processing is not required.
    2. The data subject must be provided specific information with regard to the purpose and extent of processing, including automatic processing of his or her personal data over a period of time, further processing of data for direct marketing and other commercial purpose, or processing for profiling, data sharing or research.
    3. The purpose shall be declared before collection unless it is not reasonable and practicable, in which case purpose must be declared after collection but before any other processing, provided that collection and processing of sensitive personal information or privileged information is prohibited unless specifically authorized by law or there is prior consent from data subject.
    4. The data subject must be informed of what data will be collected, the period of collection and how long the collected data will be stored.
    5. Personal data to be collected shall only be that which is necessary and compatible with declared, specified and legitimate purpose.

b. Personal data shall be processed fairly and lawfully
    1. Processing shall be in accordance with the rights of the data subject, and shall be transparent, affording data subject sufficient information as to the identity of controller and recipients of data, right to refuse or withdraw consent, or to object, and other information relevant to the processing.

2. Information provided to a data subject must always be in clear and plain language, easy to understand and easily accessible.
3. Processing must be compatible with declared, specified and legitimate purpose.
4. Processed personal data should be adequate, relevant and not excessive in relation to the declared, specified and legitimate purpose.
5. Adequate privacy and security safeguards should be in place in the processing of personal data.

c. Processing should ensure data quality
   1. Personal data should be accurate, relevant and complete with respect to the purpose of processing.
   2. Personal data shall be kept up to date when necessary for the declared, specified and legitimate purpose.
   3. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

d. Personal Data shall not be retained longer than necessary
   1. Retention of personal data shall only be until the declared, specified and legitimate purpose has been achieved or the processing relevant to the purpose has been terminated.
   2. Retention of personal data may be allowed when necessary to establish, exercise or defend legal claims, or for legitimate business purposes, or as provided by law, which must be in accordance with standards followed by the applicable industry or approved by appropriate government agency, and taking into consideration prescriptive periods.
   3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access or disclosure to any other party or the public, or prejudice to the interests of the data subjects.

e. Any authorized further processing shall have adequate safeguards. Personal data originally collected for a declared, specified or legitimate purpose may be retained longer and processed further for historical, statistical or scientific purposes, and other purpose specifically authorized by law when there are adequate safeguards for data privacy and security.
   1. Personal data kept longer than necessary for the declared, specified and legitimate purpose shall be aggregated or in

a form which does not permit identification of data subjects.

2. Personal data can not be retained in perpetuity in contemplation of a possible future use still to be determined.

Section 20. General principles for Data Sharing. Further Processing of Personal Data collected from a party other than the Data Subject shall be allowed under any of the following conditions:

a. Data sharing is specifically provided by law, where the law authorizing the sharing provides adequate safeguards for data privacy and security.

b. Data Sharing in the Private Sector shall be allowed if the data subject consents to data sharing:
   1. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships, unless the data sharing is specifically authorized by law;
   2. Data sharing for commercial purpose, including direct marketing, shall be covered by a data sharing agreement.
      (a) The data sharing agreement should put in place adequate safeguards for data privacy and security, uphold rights of data subjects and provide a system by which data subject can obtain relief for violations.
      (b) The data sharing agreement shall be subject to review of the Commission;
   3. The data subject shall be provided with the following information prior to collection or before data is shared:
      (a) Identity of all controllers or processors who will be given access to data;
      (b) Purpose of further processing;
      (c) Categories of data concerned;
      (d) Intended recipients or categories of recipients of data;
      (e) Existence of rights of data subject, including right to access and correction, and right to object;
      (f) Other information that would sufficiently notify the data subject of the extent of data sharing and manner of processing; and
   4. Further processing of shared data shall adhere to the data protection principles laid down in the Act, these Rules and other issuances of the Commission.

c. Data collected from parties other than the data subject for purpose of research shall be allowed provided the personal

data is publicly available or has the consent of the data subject for purpose of research, adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. Prior notification is required, unless a body authorized by the Commission, or by law, has approved the research proposal. The proposed research shall provide a system by which the data subjects can exercise their rights and obtain relief without compromising research integrity.

d. Data Sharing for purpose of a public function or provision of a public service in government agencies shall be allowed provided the personal information controller sharing information under its control or custody with another personal information controller enters into a data sharing agreement. The Commission should be notified prior to data sharing.

Rule V. Lawful Processing of Personal Data

Section 21. Criteria for Lawful Processing of Personal Information. Processing of personal information is allowed unless prohibited by law. For processing to be lawful:

a. The data subject must have given his or her consent prior to collection, or as soon as practicable and reasonable.
b. It involves processing of personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering into a contract.
c. The processing of information is necessary to comply with obligations imposed on the personal information controller by law or rules.
d. The processing of the personal information of a data subject is necessary to protect his or her vitally important interests, including life and health.
e. The processing of personal information is to the extent necessary to respond to national emergency or to comply with the requirements of public order and safety as prescribed by law.
f. The processing of personal information is to the extent necessary for the performance of the constitutional or statutory mandate of a public authority.
g. The processing must be necessary to pursue the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require

protection under the Philippine Constitution. The interest is legitimate if it relates to a compelling benefit of both the personal information controller and the public with minimal impact on the rights of data subject.

Section 22. Sensitive Personal Information and Privileged Information. The processing of sensitive personal and privileged information is prohibited. It shall be allowed only in the following cases:

a. Consent is given pursuant to a declared, specified and legitimate purpose by data subject prior to the processing of sensitive personal information, or by parties to the exchange prior to processing of privileged information.
b. The processing of the sensitive personal or privileged information is in accordance with existing laws and regulations that does not require consent of data subject for processing, and which guarantees the protection of the sensitive personal information and the privileged information.
c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing.
d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:
   (1) Processing is confined and related to the bona fide members of these organizations or their associations;
   (2) The sensitive personal information are not transferred to third parties; and
   (3) Consent of the data subject was obtained prior to processing.
e. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured. The use, access to, disclosure and other processing of personal data for purposes other than for medical treatment of the data subject requires consent.
f. The processing concerns such sensitive personal or privileged information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority based on a specific constitutional or statutory provision.

Section 23. Extension of Privileged Communication. Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

When the Commission inquires upon communication claimed to be privileged, the Personal Information Controller should prove the nature of the communication in an executive session. Should the communication be determined as privileged, it shall be excluded from evidence, and the contents of the communication shall not form part of the records of the case. This rule will apply unless the privileged communication is itself the subject of the breach or privacy concern, in which case the privileged communication will be subject of investigation, only to the extent necessary for purposes of investigation without including the contents of the communication in the records.

Section 24. Surveillance of Suspects and Interception of Recording of Communications. The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended to include the condition that the processing of personal data for purpose of surveillance and interception of recording of communications must comply with the Data Privacy Act, including adherence to the principles of transparency, proportionality and legitimate purpose.

Rule VI. Security Measures for Data Protection

Section 25. Data Privacy and Security. The personal information controller shall put in place organizational, physical and technical security measures for data protection, including policies for evaluation, monitoring and review of operations and security risks. The same obligation shall be required from personal information processors engaged by the personal information controller to process personal data on its behalf.

These measures shall aim to maintain the availability, integrity and confidentiality of personal data, and prevent negligent, unlawful or fraudulent processing, access and other interference, use, disclosure, alteration, loss and destruction of personal data.

The guidelines in the succeeding sections shall be implemented by any natural or juridical person involved in the processing of data, which shall also be included in the privacy and security policy of the company.

Section 26. Guidelines for organizational security measures shall include:

a. Accountable Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall be accountable for ensuring compliance with applicable laws and regulations for protection of data privacy and security. These accountable officers may be a compliance officer, privacy officer, information officer or a data protection officer, provided that the officer or officers so designated shall manage the privacy and security aspect in the different areas of the operations, and shall plan, implement and evaluate policies and programs for data privacy and security.

b. Accountability and Transparency. Any natural or juridical person or other entity involved in the processing of personal data shall sufficiently describe its data processing system, and identify duties and responsibilities of those who will have access to personal data. The privacy policy should include:
   1. Information about the purpose of collection and processing of personal data, including purpose of any intended future processing, data sharing, access or disclosure;
   2. Information about the data flow within the organization, from the time of collection, processing, retention and disposal of personal data;
   3. A description of data processing system and the physical and technical security measures being implemented at every stage of processing;
   4. A governance and accountability structure for the processing of personal data, which shall identify the duties and responsibilities of those directly involved in the processing of personal data, including identification of the data protection officer or any other individual or individuals accountable for ensuring compliance with applicable laws and regulations for protection of data privacy and security.

c. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall have the responsibility of selecting and supervising its employees, agents or representatives, particularly those who will have access to personal data. It must implement or impose:

1. Procedures for hiring of employees involved in the processing of personal data, which shall include an assessment of the potential employee's capacity and competence to perform the functions of the position being applied for and evaluation of other conditions that may impact the fitness of the applicant to handle and access personal data;
2. Capacity building, orientation or training programs for employees regarding privacy and security policies;
3. Duty of Strict confidentiality on individuals involved in the processing of personal data, which should form part of the terms of engagement or employment and which shall continue even after the individual leaves the service, transfers to another position or upon termination of employment or contractual relations;
4. A formal process for ending a person's employment or a user's access so that inappropriate access to personal data does not occur;
5. Procedure for incident reporting, investigations and sanctions for violation of the Act, these rules, or other company policy.

d. Policy for Collection and Processing of Personal Data. Any natural or juridical person or other entity involved in the processing of personal data shall develop, implement and review:
   1. A protocol and design for collection of personal data, including procedures for obtaining consent, and other rules relating to the effective period of any consent given, when applicable;
   2. Policy and procedure for data subjects to exercise their rights under the Data Privacy Act, including the right of notification, access, correction, or withdrawal of any consent previously given pertaining to the processing of their personal data;
   3. An access management policy which shall include a process for accreditation and authentication of authorized users granted access to the system, policies to implement role-based access controls, and maintenance of a secure user record database;
   4. Procedures to limit the processing of data, to ensure that it is only to the extent necessary to the declared and specified purpose at time of collection;
   5. Policy and procedure to monitor the system for security breach or any other irregularity that may compromise the availability, integrity and confidentiality of the personal data, including a process for identifying and accessing

reasonably foreseeable vulnerabilities in its computer networks;

6. A protocol to be followed in case of security incident or technical problems, including procedures for prevention, investigation, correction and mitigation of any damage that might result due to a security incident or security breach;
7. Data retention schedule approved by appropriate body, when applicable, including erasure or disposal of records.

e. Contracts with processors or third parties. The personal information controller must further ensure that personal information processors or third parties processing personal information on its behalf shall implement the security measures required by the Act, these Rules and other issuances of the Commission. Contracts with an information processor or any third party shall ensure continued protection of personal data, which may include stipulations providing the minimum standards for data protection and data management, restrictions on access, use and disclosure of personal data, and provisions on damages.

f. Review and Monitoring. Any natural or juridical person or other entity involved in the processing of personal data shall adopt a quality management program and put in place procedures for review and monitoring, including:
   1. Procedure for security incident reporting, including notification of the National Privacy Commission in cases of security breach;
   2. Procedures for implementing quality management and internal audits within the organization or agency;
   3. Policy for documentation, regular review, evaluation and updating of the privacy and security policies and practices.

Section 27. Guidelines for Physical security measures shall include:

a. The personal information controller shall implement policies and procedures to limit physical access to its facility and work stations, including guidelines which specify proper use of and access to workstations and electronic media.
b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to public.
c. Policies and procedures shall be implemented to monitor and limit activities in the room or workstation. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure

that only the individuals actually performing official duties shall be in the room or work station, at any given time.

d. The personal information controller should implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data.
e. Policies and procedures to prevent mechanical destruction of files and equipment shall be in place. The room and workstation shall in so far as may be practical be secured against natural disasters, power disturbances, external access and other similar threats.

Section 28. Guidelines for Technical security measures shall include:

a. Personal information controllers shall have in place technical and logical security measures for data protection, intended to safeguard the availability, integrity and confidentiality of personal data.
b. Personal data in a computer network should be protected against risks such as accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder functioning or availability of system, and unauthorized access transmitted over an electronic network. Regular assessment for vulnerabilities in its computer systems should be conducted.
c. Hardware, software, and procedural mechanisms to record and examine access and other activity in information systems containing personal data, including the monitoring and tracking of any alterations, deletions or additions made to records shall be implemented.
d. Technical Security measures such as data encryption, during storage and while in transit, authentication process, and other measures to control and limit access to electronic data should be in place.

Section 29. Appropriate Level of Security. The Commission shall monitor compliance of natural or juridical person or other body involved in the processing of personal data on their security measures based on the guidelines provided in these Rules and subsequent issuances of the Commission. The determination of the appropriate level of security measures must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation, and shall be updated by the Commission in separate issuances, as

may be necessary, taking into account the most appropriate standard recognized by the information and communications technology industry and data privacy best practices.

Rule VII. Data Privacy and Security in Government.

Section 30. Responsibility of Heads of Agencies. All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to these Rules and other issuances of the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein. The Commission shall monitor agency compliance and may recommend the necessary action in order to satisfy the minimum standards.

Section 31. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.

a. On-site and Online Access.
    1. No employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency. The source agency is the agency who originally collected the personal data.
    2. A source agency shall strictly regulate access to sensitive personal data under its custody or control, particularly when it allows online access, and shall grant a security clearance only when the performance of official functions or provision of a public service directly depends on and can not otherwise be performed unless online access is allowed to the agency personnel.
    3. Online access to sensitive personal information shall be allowed, upon approval of the head of the source agency, subject to the following:
        (a) An information technology governance framework has been designed and implemented.
        (b) Sufficient organizational, physical and technical security measures are in place.
        (c) The agency is capable of protecting sensitive personal information in accordance with best data privacy practices and standards recognized by information and communication technology industry.

(d) The agency personnel given online access has a security clearance which provides access limited only to that information needed for the performance of official functions.

b. Off-site access.
   1. Sensitive personal information maintained by an agency may not be transported or accessed from a location off government property whether by its agent or employee unless the head of agency has ensured implementation of privacy policies and appropriate security measures. A request for such transportation or access is submitted to and approved by the head of the agency, which must include proper accountability structures in the processing of data.
   2. The head of agency shall approve requests for off-site access in accordance with the following guidelines:
      (a) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;
      (b) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time, subject to the succeeding paragraph. Exceptions to this limitation may be approved by the head of source agency if necessary to a public function or provision of public service subject to the same conditions for approving online access.
   3. Encryption. Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

Section 32. Implementation of Security Requirements. Notwithstanding the effective date of these Rules, the requirements in the preceding paragraphs shall be implemented before any off-site or online access request is approved. The Commission shall be notified of any data sharing agreement between a source agency and another government agency.

Section 33. Applicability to Government Contractors. In entering into any contract that may involve accessing or requiring sensitive

personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal data processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding sections, in the same manner as agencies and government employees comply with such requirements.

Rule VIII. Rights of Data Subject

Section 34. Rights of the Data Subject. The data subject is entitled to the following rights:

a. Right to be informed.
    1. The data subject has a right to know whether personal data pertaining to him or her shall be, are being or have been processed, and whether the processing is partly or wholly automatic. In cases where the collection of data shall be done over a period of time, including automatic collection of categories of data, the data subject must be notified in clear and simple language of this fact, and his or her express consent must be obtained prior to the processing.
    2. The data subject shall be notified and furnished the information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:
        (a) Description of the personal data to be entered into the system;
        (b) Purposes for which they are being or are to be processed, including processing for direct marketing or historical, statistical or scientific purpose;
        (c) Scope and method of the personal data processing;
        (d) The recipients or classes of recipients to whom they are or may be disclosed;
        (e) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
        (f) The identity and contact details of the personal data controller or its representative;
        (g) The period for which the information will be stored; and
        (h) The existence of their rights including the right to access, correction, and object to the processing, as well

as the right to lodge a complaint before the Commission.

b. Right to object. The data subject shall be notified and given an opportunity to object or withhold consent to processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph, unless the change refers to processing of personal data in the following cases:
   1. The personal data is needed pursuant to a subpoena;
   2. 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 to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
   3. When the information is being collected and processed as a result of a legal obligation.

c. Right to Access. The data subject has the right to reasonable access to, upon demand, of the following:
   1. Contents of his or her personal data that were processed;
   2. Sources from which personal data were obtained;
   3. Names and addresses of recipients of the personal data;
   4. Manner by which such data were processed;
   5. Reasons for the disclosure of the personal data to recipients;
   6. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
   7. Date when his or her personal data concerning the data subject were last accessed and modified; and
   8. The designation, or name or identity and address of the personal information controller.

d. Right to correct. The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data 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 data shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject.

e. Right to Rectification, Erasure or Blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.
   1. This right may be exercised upon discovery and substantial proof that:
      (a) The personal data is incomplete, outdated, false, or unlawfully obtained;
      (b) The personal data is being used for purpose not authorized by the data subject;
      (c) The personal data is no longer necessary for the purposes for which they were collected;
      (d) The personal data concerns private information that is prejudicial to data subject unless matter of public concern, part of fair and true reporting or otherwise justified; or
      (e) The personal information controller or processor violated the rights of the data subject.

   2. The data subject may request the personal information controller to notify third parties who have previously received such processed personal data.

f. Right to damages. The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data or any injury that may have been incurred due to a violation of his or her rights and freedoms as data subject.

Section 35. Transmissibility of Rights of the Data Subject. The lawful heirs and assigns of the data subject may invoke the rights of the data subject for which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

Section 36. Right to Data Portability. The data subject shall have the right, where personal data is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have greater control over personal data being processed for commercial purpose, without compromising

national security matters and intelligence information, trade or industrial secrets, integrity of research, and other matters which are deemed confidential under the law. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

Section 37. Limitation on Rights. The immediately preceding sections on the transmissibility of the rights of data subjects and the right to data portability shall not be applicable if the processed personal data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, that the personal data shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the said sections are not applicable to processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject, provided that the exercise of the data subjects of his or her rights shall not compromise the investigation.

Rule IX. Data Breach Notification.

Section 38. Data Breach Notification.

a. The Commission and affected data subjects shall be notified within 72 hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a security breach has occurred. Security breach subject of notification under this subsection shall be 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.
b. Depending on the nature of the incident, or if there is delay or failure to notify, the Commission may investigate the circumstances surrounding the information security breach. Investigations may include on-site examination of systems and procedures.

Section 39. Contents of Notification. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. The notification to the data subject should also include measures taken to reduce negative

consequence, the authorities or contact details where the data subject can obtain additional information about the breach, and any assistance to be provided the affected data subjects.

Section 40. Delay of Notification. 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.

a. 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.
b. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.
c. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Section 41. Breach Report.

a. The personal information controller shall notify the Commission by submitting a report, whether written or electronic, containing the required information. The personal information controller shall also include in the report the name of a designated representative and his or her contact information. In case of submission by electronic mail, the personal information controller shall ensure secure transmission.
b. All security incident or security breach shall be documented even if not covered by the notification requirements. For security breach, these should include the facts surrounding the incidents, effects and the remedial actions taken. For other security incidents, aggregated data shall constitute sufficient compliance. These reports shall be made available upon demand. An electronic summary shall be submitted to the Commission annually.

Section 42. Procedure for Notification. The Procedure for security breach notification shall be in accordance with the Act and these Rules, and any other issuance of the Commission.

Rule X. Outsourcing and Subcontracting Agreements.

Section 43. Subcontract of Personal Data. A personal information controller may subcontract the processing of personal data,

provided that the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act and other applicable laws, these Rules and other issuances for processing of personal data.

Section 44. Agreements for Outsourcing. Agreements for outsourcing or subcontracting shall include the following:

a. Subject and duration of work;
b. The extent, type and purpose of data processing;
c. Technical and organizational measures to be taken;
d. The rectification, erasure and blocking of data;
e. The processor's obligations, particularly with regard to monitoring;
f. Rights regarding subcontracting;
g. The controller's monitoring rights;
h. The subcontractor's notification obligations;
i. The extent of the controller's authority to issue instructions to the processor;
j. The return and/or erasure of data by the processor at the conclusion of the work;
k. The geographic location/s at which the processing under the subcontracting agreement will be performed.

Section 45. Duty of personal information processor. The personal information processor shall comply with all the requirements of this Act and other applicable laws, in addition to obligations provided in the agreement with a personal information controller. These shall include the duty to put in place adequate safeguards for data privacy and security, to comply with standards for organizational, physical and technical security measures, and to uphold the rights of data subjects.

Rule XI. Registration and Compliance Requirements

Section 46. Enforcement of the Data Privacy Act. Pursuant to the mandate of the Commission to administer and implement the Act, and to ensure compliance of personal information controllers with its obligations under the law, the Commission requires:

a. Registration of personal data processing systems operating in the country, including the personal data processing system of contractors and its employees entering into contracts with government that involves accessing or requiring sensitive personal information from one thousand (1,000) or more individuals;

b. Notification of the Commission prior to data sharing if the personal data to be shared is under control or custody of the government;
c. Annual report on documented security incidents; and
d. Compliance with other requirements that may be provided in other issuances of the Commission.

Section 47. Registration of Personal Data Processing Systems. Any personal information controller shall register with the Commission their processing operations and data processing systems.

a. The contents of registration shall include:
    1. The name and address of the controller and of his representative, if any, including their contact details;
    2. The purpose or purposes of the processing;
    3. A description of the category or categories of data subject and of the data or categories of data relating to them;
    4. The recipients or categories of recipient to whom the data might be disclosed;
    5. Proposed transfers of data outside the Philippines;
    6. A description of privacy and security measures for data protection;
    7. Name/address/contact details of the compliance or accountable officer;
    8. Description of the information and communications system;
    9. Copy of all policies relating to data governance, data privacy, and information security; and
    10. Attestation to all certifications attained that are related to information and communications processing.

b. In case of complaints or violations of the Act or these Rules, the failure to register shall be taken into consideration in imposing the fine or penalty.
c. The procedure for registration shall be in accordance with these Rules and the issuances of the Commission.

Registration of personal data processing systems operating in the country will be required when processing of personal data involves one thousand (1,000) or more individuals. (being reviewed)

Section 48. Notification for automatic Processing Operations. The personal information controller shall notify the Commission the carrying out any wholly or partly automatic processing operations or set of such operations intended to serve a single purpose or several related purposes when the automatic processing becomes

the sole basis of making decisions about a data subject and when the decision would significantly affect the data subject.

a. The contents of notification should sufficiently detail the following information:
    1. Purpose of processing;
    2. Data or categories of data to undergo processing;
    3. Category or categories of data subject;
    4. The recipients or categories of recipient to whom the data are to be disclosed;
    5. The length of time the data are to be stored;
    6. Methods and logic utilized for automated processing
    7. Any decisions relating to the data subject that would be made on the basis of processed data or that would affect adversely the rights and freedoms of data subject.
b. The Commission shall be given the identity of contact persons from the Personal Information controller and any other body involved in processing of personal data with their contact details, and which shall immediately be updated in case of changes.
c. No decision with legal effects concerning the data subject shall be made solely on the basis of automated processing, unless data subject consents.

Section 49. Prior Notification of Data Sharing Agreements. The personal information controller seeking to enter into a data sharing agreement with a natural or juridical person or other body with control or custody of personal data shall enter into a formal data sharing agreement.

a. Prior notification of the Commission shall be required in cases where data sharing involves personal data under control and custody of any government body, unless the proposed data sharing is specifically authorized by law.
b. Data sharing for purpose of research shall require prior notification unless a body authorized by the Commission, or by law, has approved the research proposal.
c. Data Sharing should be in accordance with these Rules and other issuances of the Commission.

Section 50. Review by the Commission. The following are subject to review or inspection of the Commission, upon its own initiative or upon complaint:

a. Compliance by a personal information controller or personal information processor with the data privacy act, these Rules and other issuances of the Commission;
b. Compliance with the requirement of putting in place adequate safeguards for data privacy and security;

c. Any data sharing agreement, outsourcing contract and similar contracts involving processing of personal data, and its implementation;
d. Any off-site or online access to sensitive personal data in government allowed by head of agency;
e. Processing of personal data for research purpose, public function, or commercial activities;
f. Any reported violation of the rights and freedoms of data subject;
g. Other matters necessary to ensure effective implementation of the Act, these Rules and other issuances of the Commission.

Rule XII. Rules on Accountability

Section 51. Accountability for Transfer of Personal Information. Each personal information controller is responsible for personal data under its control or custody, including information that have been transferred to a personal information processor or 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 personal information processor or a third party.
b. The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual or individuals so designated shall be made known to any data subject upon request.

Section 52. Accountability for violation of the Act, these Rules and other issuances.

a. Administrative Liability. Any natural or juridical person or other body involved in the processing of personal data, and who fails to comply with the requirements of the Act, these Rules and other issuances, shall be liable for the violation, and the corresponding penalty or fine.
b. Civil Liability. In cases where a data subject files a complaint for violation of his or her rights as data subject, and for any injury suffered as a result of the processing of his or her personal data, the liability shall be imposed on the personal information controller. The personal information processor,

compliance officer, employees or agents, depending on the circumstance, may be held jointly liable with personal information controller for the award of indemnity to the data subject, without prejudice to any other sanction, fine or penalty that the Commission may impose.

c. Criminal Liability. In case of criminal acts and corresponding personal penalties, the person who committed the unlawful act or omission based on substantial evidence shall be recommended for prosecution. The personal information controller or personal information processor is the offender if the commission of the unlawful act or omission was committed pursuant to a policy, order or instruction of the personal information controller or personal information processor, or if the crime is one defined under the Act as being committed by the personal information controller or processor. 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.

Rule XIII. Penalties

Section 53. 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 who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.
b. The unauthorized processing of sensitive personal information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process sensitive personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

Section 54. 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 who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

b. Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to sensitive personal information without being authorized under this Act or any existing law.

Section 55. 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 who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.
b. The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the sensitive personal information of an individual in an area accessible to the public or has otherwise placed the sensitive personal information of an individual in its container for trash collection.

Section 56. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.

a. The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

b. The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine 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 processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

Section 57. 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 who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

Section 58. Concealment of Security 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 persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f) of the Data Privacy Act, intentionally or by omission conceals the fact of such security breach.

Section 59. Malicious Disclosure. Any personal information controller or personal information processor 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 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 a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

Section 60. Unauthorized Disclosure.

a. Any personal information controller or personal information processor 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, shall be subject to 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 One million pesos (Php1,000,000.00).

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 imprisonment ranging from three (3) years to five (5) 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).

Section 61. Combination or Series of Acts. Any combination or series of acts as defined in Sections 53 to 60 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

Section 62. 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 55 and 56 of these Rules, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

Section 63. Large-Scale. The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal data of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

Section 64. Offense Committed by Public Officer. When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied.

Section 65. Restitution. Pursuant to the exercise of its quasi-judicial functions, the Commission shall award indemnity to

an aggrieved party on the basis of the provisions of the New Civil Code. Any complaint filed by a data subject shall be subject to payment of filing fees unless data subject is an indigent.

Section 66. Fines and Penalties. Violations of the Data Privacy Act, these Rules, other issuances and orders of the Commission, shall, upon notice and hearing, be subject to cease and desist orders, temporary or permanent ban on the processing of personal data, compliance and enforcement orders or payment of fines in accordance with a schedule to be published by the Commission.

Rule XIV. Miscellaneous Provisions

Section 67. Appeal. Appeal from decisions of the Commission shall be to the proper courts as may be prescribed by law or rules.

Section 68. Period for Compliance. Any natural or juridical person or other body involved in the processing of personal data shall comply with the personal data processing principles and standards already laid out in the Data Privacy Act.

Personal information controllers and processors shall be given one year from the effectivity of these rules to register their data processing systems or notify their automatic processing operations to the Commission. Any subsequent issuance of the Commission including those that implement specific standards for data portability, secure encryption, or other security measures shall provide the period for its compliance.

For a period of one year from the effectivity of these Rules, a personal information controller and/or processor may apply for extension of time to comply with the issuances of the Commission, but only for good cause shown, and subject to the discretion of the Commission.

Section 69. Interpretation. Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner that would uphold the rights and interests of the individual about whom personal data is processed.

Section 70. 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 71. Repealing Clause. Except as otherwise expressly provided in the Act or these Rules, all other laws, decrees,

executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

Section 72. Effectivity Clause. This Act shall take effect on August 10, 2016, after its publication in at least two (2) national papers of general circulation.