Data Privacy Act (RA 10173)
Bar Review Notes (2019)

Prepared by: Atty. Arnel D. Mateo

The Data Privacy Act (Act) protects the right to privacy of an **individual** with regard to his personal data. It imposes upon any person processing personal data the obligation to implement security measures aimed at ensuring the confidentiality, integrity, and availability of an individual's personal data.

A. Personal Information vs. Sensitive Personal Information

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

  (Ex. Name, photo, signature, biometric data)

- when put together with other information would directly and certainly identify an individual.

  (Ex. username, password, IP address, location, cookies, birthday)

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.

Other important terms to remember:

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

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 personal, 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;

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

Data sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;

Personal information controller refers to a person or organization who controls the collection, holding, 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:

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

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

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 data pertaining to a data subject.

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, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

B. Scope

Application:

The Act and these Rules apply to the processing of personal data by any natural and juridical person in the government or private sector. They apply to an act done or practice engaged in and outside of the Philippines if:

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; or

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, such as, but not limited to, the following:

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 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 data;

5. An entity that carries on business in the Philippines;

6. An entity that collects or holds personal data in the Philippines.

This Act does not apply to the following:

(a) 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:

(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;

(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) Personal information processed for journalistic, artistic, literary or research purposes;

(e) 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) 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.

***Protection afforded to Data Subjects*.**

a. Unless directly incompatible or inconsistent with the preceding sections in relation to the purpose, function, or activities the non-applicability concerns, the personal information controller or personal information processor shall uphold the rights of data subjects, and adhere to general data privacy principles and the requirements of lawful processing.

b. The burden of proving that the Act and these Rules are 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 any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

Protection Afforded to Journalists and Their Sources. – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter.

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

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

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

(1) A contract is entered in the Philippines;

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

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

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

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

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

C. Processing of Personal Information

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

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

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. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

General principles in collection, processing and retention.

a. Collection must be for a declared, specified, and legitimate purpose.

1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

2. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.

3. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.

4. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

b. Personal data shall be processed fairly and lawfully.

1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.

2. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.

3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.

4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.

c. Processing should ensure data quality.

1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.

2. 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 for as long as necessary:

(a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;

(b) for the establishment, exercise or defense of legal claims; or

(c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

2. Retention of personal data shall be allowed in cases provided by law.

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 the interests of the data subjects.

e. Any authorized further processing shall have adequate safeguards.

1. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.

2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

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 shall be allowed when it is expressly authorized by law: *Provided*, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.

b. Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:

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;

2. Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.

(a) The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.

(b) The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject;

3. The data subject shall be provided with the following information prior to collection or before data is shared:

(a) Identity of the personal information controllers or personal information processors that will be given access to the personal data;

(b) Purpose of data sharing;

(c) Categories of personal data concerned;

(d) Intended recipients or categories of recipients of the personal data;

(e) Existence of the rights of data subjects, including the right to access and correction, and the right to object;

(f) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

4. Further processing of shared data shall adhere to the data privacy 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 when the personal data is publicly available, or has the consent of the data subject for purpose of research: Provided, that 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. The rights of the data subject shall be upheld without compromising research integrity.

d. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered a data sharing agreement.

1. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security.

2. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject.

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

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

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

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

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

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

(f) The processing is necessary for the purposes of 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.

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

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or 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 such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That 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 information is ensured; or

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

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

Extension of Privileged Communication. – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process.

***Surveillance of Suspects and Interception of Recording of Communications*.** The processing of personal data for the purpose of surveillance, interception, or recording of communications shall comply with the Data Privacy Act, including adherence to the principles of transparency, proportionality, and legitimate purpose.

D. Rights of data Subject

Rights of the Data Subject. – The data subject is entitled to:

a. Right to be informed.

1. The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.

2. The data subject shall be notified and furnished with 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 will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;

(c) Basis of processing, when processing is not based on the consent of the data subject;

(d) Scope and method of the personal data processing;

(e) The recipients or classes of recipients to whom the personal data are or may be disclosed;

(f) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

(g) The identity and contact details of the personal data controller or its representative;

(h) The period for which the information will be stored; and

(i) The existence of their rights as data subjects, 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 have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. 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 data, unless:

1. The personal data is needed pursuant to a subpoena;

2. 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. 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, 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, if any;

6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects 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, name or identity, and address of the personal information controller.

d. Right to rectification. 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 has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or 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 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 of any of the following:

(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 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 data 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;

(g) The personal information controller or personal information processor violated the rights of the data subject.

2. The personal information controller may notify third parties who have previously received such processed personal information.

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, taking into account any violation of his or her rights and freedoms as data subject.

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.

Right to Data Portability. – The data subject shall have the right, where personal information 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 Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

Non-Applicability. – The immediately preceding sections are not applicable if the processed personal information 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 information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.