DATA PRIVACY ACT OF 2012
(R.A. NO. 10173)

- **Policies of the State**
  - It is the policy of the state to protect the fundamental human rights of privacy, of communication while ensuring free flow of information to promote innovation and growth.
  - The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.
  - **Data privacy** refers to the right while data protection refers to the means to implement the right data privacy.

- **Definition of Terms**
  - **Commission** shall refer to the **National Privacy Commission** created by virtue of this Act.
  - **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 personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
  - **Data subject** refers to an individual whose personal information is processed.
  - **Direct marketing** refers to communication by whatever means of any advertising or marketing materials which is directed to particular individuals.
  - **Filing system** refers to any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.
  - **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.
  - **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.
  - **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 Personal information controller **excludes** the following:
    - ✓ A person or organization who performs such functions as instructed by another person or organization; and
    - ✓ An 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.
  - **Privileged information** refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
  - **Sensitive personal information** refers to personal information about the following:
    - ✓ About an individual's race, ethnic origin, marital status, age, color; and religious, philosophical or political affiliations;
    - ✓ 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;
    - ✓ 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
    - ✓ Specifically established by an executive order or an act of Congress to be kept classified.

Scope of Data Privacy Act

- The law applies to the **processing of all types of personal information** and to any **natural** and **juridical** person involved in personal information processing including those personal information controllers and processors who, although, not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: Provided, That the requirement of Section 5 are complied with Section 5 affords protection 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 reports of any newspaper, magazine or periodical 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.

Exceptions to Coverage of Data Privacy Act

- **The law does not apply to the following:**
  - 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:
    - ✓ The fact that the individual is or was an officer or employee of the **government institution**.
    - ✓ The title, business address and office telephone number of the individual.

- ✓ The classification, salary range and responsibilities of the position held by the individual.
- ✓ The name of the individual on a document prepared by the individual in the course of employment with the government.

- 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.

- 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.

- Personal information processed for **journalistic, artistic, literary or research** purposes.

- **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 for 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).

- **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.

- **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.

Extraterritorial Application of Data Privacy Act

- The law applies to an act done or practice engaged in and outside of the Philippines by an entity if:

  - The act, practice or processing relates to **personal information about a Philippine citizen or a resident.**

  - 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:
    - A contract is entered in the Philippines.
    - A juridical entity unincorporated in the Philippines but has central management and control in the country.
    - 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.

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

National Privacy Commission

- **Functions of National Privacy Commission**

  - **Ensure compliance** of personal information controllers with the provisions of this Act.
  - **Receive complaints**, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: Provided, that in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act.

  - **Issue cease and desist orders**, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.

  - **Compel or petition of any entity**; government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy.

  - **Monitor the compliance** of other 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 information pursuant to this Act.

  - **Coordinate** with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information to the country.

  - **Publish on a regular basis a guide to all laws** relating to data protection.

  - **Publish a compilation of agency system** of records and notices, including index and other finding aids.

  - **Recommend to the Department of Justice (DOJ)** the **prosecution** and imposition of penalties specified in Sections 25 to 29 of this Act.

  - **Review, approve, reject or require modification of privacy codes** voluntarily adhere to by personal information controllers: Provided, that the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: Provided, further, that such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: Provided, finally. That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act.

  - **Provide assistance** on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person.

  - **Comment on the implication** on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws.

- **Propose** legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary.

- **Ensure property and effective coordination** with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection.
-
- **Negotiate and contract** with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws.

- **Assist Philippine companies** doing business abroad to respond to foreign privacy or data protection and regulations.

- Generally perform such acts as may be **necessary to facilitate cross-border enforcement** of data privacy protection.

○ **Confidentiality in National Privacy Commission** – The National Privacy Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

○ **Organization Structure of National Privacy Commission (NPC)**

- **Composition** – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as **Chairman** of the Commission. The Privacy Commissioner shall be assisted by **two (2) Deputy Privacy Commissioners**, one to be responsible for Data processing Systems and one to be responsible for Policies and Planning.

- Appointment **to** the NPC – the Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines. Vacancies in the Commission shall be filled in the same manner in which the original appointments were made.

- **Term of Office** – The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall have a term of **three (3) years**, and may be reappointed for another term of three (3) years.

- **Qualifications of NPC Commissioners**

  ✓ The Privacy of 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 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.

- **Liability of NPC Commissioners**

  ✓ As a general rule, 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 NPC for reasonable cost of litigation.

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. It is the duty of personal information controller to ensure implementation of personal information processing principles set out below. The following are the general data privacy principles:

  ✓ Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only.

  ✓ Personal information must be processed fairly and lawfully.

  ✓ Personal information must be accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

  ✓ Personal information must be adequate and not excessive in relation to the purposes of which they are collected and processed.

  ✓ Personal information must be retained only for as long as necessary for the fulfillment of the purposes for which the data were obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law.

  ✓ Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, that adequate safeguards are guaranteed by said laws authorizing their processing.

○ **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:

  ✓ The data subject has given his or her consent;

  ✓ 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;

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

  ✓ 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

  ✓ The processing is necessary for the purposes of the legitimate interest pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except such interest are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

- **Sensitive Personal Information and Privileged Information –** As a general rule, the processing of sensitive personal information and privileged information shall be prohibited. However, the following are the exceptional cases wherein processing of sensitive personal information and privileged information may be allowed:

  - 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;

  - 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;

  - 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 consent prior to the processing;

  - 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;

  - 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

  - 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 and Inadmissibility of Privileged Information as Evidence** – 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.

Rights of Data Subject

- **Right to be informed** whether personal information pertaining to him or her shall be, are being or have been processed;

  - **Right to be furnished** the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

    - ✓ Description of the personal information to be entered into the system.
    - ✓ Purposes for which they are being or are to be processed.
    - ✓ Scope and method of the personal information processing.
    - ✓ The recipients or classes of recipients to whom they are or may be disclosed.
    - ✓ Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized.
    - ✓ The identity and contact details of the personal information controller or its representative.
    - ✓ The period for which the information will be store; and
    - ✓ The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

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

  - **Right to have reasonable access** to, upon demand, the following:
    - ✓ Contents of his or her personal information that were processed.
    - ✓ Sources from which personal information were obtained.
    - ✓ Names and addresses of recipients of the personal information.
    - ✓ Manner by which such data were processed.
    - ✓ Reasons for the disclosure of the personal information to recipients.
    - ✓ 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.
    - ✓ Date when his or her personal information concerning the data subject were last accessed and modified.
    - ✓ The designation, or name or identity and address of the personal information controller.

  - **Right to dispute the inaccuracy or error** in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retraced information by recipients thereof; Provided, that the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject.

  - **Right to suspend, withdraw or order the blocking, removal or destruction** of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdate, false, unlawfully obtained, used for unauthorized purposes or are not longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information.

- **Right to indemnified for any damages** sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.
  - ✓ **Transmissibility of Rights of 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 above.

- **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 of the Rights of Data Subject –** The data privacy subject rights are not applicable if the processed 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.

Security of Personal Information

- The following are the **internal control measures** to be implemented by the personal information controller to secure personal information:

  - The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

  - The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

  - The determination of the appropriate level of security under this section 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. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:
    - ✓ Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability.
    - ✓ A security policy with respect to the processing of personal information.
    - ✓ A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.
    - ✓ Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

  - The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

  - The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

  - The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identify 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.

  - 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. 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 communication system.

    - ✓ 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.
    - ✓ 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.
    - ✓ The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Accountability of Personal Information Controller for Transfer of Personal Information

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

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

- 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(s) so designated shall be made known to any data subject upon request.

- - END - -

DATA PRIVACY ACT

1. It 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
   a. Public information
   b. Private information
   c. Personal information
   d. Individual information

2. It refers to an individual whose personal information is processed
   a. Data object
   b. Data prestation
   c. Data subject
   d. None of the above

3. It refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her
   a. Consent of the data subject
   b. Object of the data subject
   c. Cause of the data subject
   d. None of the above

4. [SKIP]

5. It 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
   a. Private information controller
   b. Personal information controller
   c. Public information controller
   d. Individual information controller

6. It refers to any natural or juridical person qualified to act as such under the Data Privacy Act of 2012 to whom a personal information controller may outsource the processing of personal data pertaining to a data subject
   a. Private information controller
   b. Public information controller
   c. Individual information controller
   d. Personal information controller

   Note: Answer should be Personal information processor
   Rationale: Data Privacy Act, Sec. 3 (i) Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

7. Which of the following is considered a sensitive personal information?
   a. Information about an individual's business, company, business venture and profitable transactions
   b. Information about an individual's Facebook public profile picture and display photo
   c. Information about an individual's Instagram public account and public twitter account
   d. Information about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations

8. Which of the following is not considered a sensitive personal information?
   a. Information 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
   b. Information 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
   c. Information specifically established by an executive order or an act of Congress to be kept classified
   d. Information about the platform of a candidate for national elective position that is discussed in a public debate televised in national television network

9. It refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication
   a. Confidential information
   b. Privileged information
   c. Sensitive information
   d. Personal information

10. Data Privacy Act applies to:
    Statement I: The processing of all types of personal information
    Statement II: To any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

11. Data Privacy Act does not apply to
    a. 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
    b. 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
    c. Personal information processed for journalistic, artistic, literary or research purposes
    d. 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
    e. All of the above

12. Data Privacy Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:
    Statement I: The act, practice or processing relates to personal information about a Philippine citizen or a resident
    Statement II: 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
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

13. Under the Data Privacy Act, personal information must be
    a. Processed unfairly and illegally
    b. Inadequate and excessive in relation to the purposes for which they are collected and processed
    c. Retained as long as possible despite the retention period necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law
    d. Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection and later processed in a way compatible with such declared, specified and legitimate purposes only

14. 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. Which is not one of the conditions?
    a. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject on in order to take steps at the request of the data subject prior to entering into a contract
    b. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject
    c. The data subject need not necessarily give his or her consent
    d. The processing is necessary to protect vitally important interests of the data subject, including life and health

    Note: According to section 12 of DPA, consent is only one of the several possible conditions that allows for lawful processing of personal information. So, it seems that consent need not actually be given.

15. 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 on in the case of privileged information, all parties to the exchange have given their consent prior to processing
    b. 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
    c. 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 f personal information is ensured
    d. All of the above

16. The following are the rights of the data subject, except
    a. Be informed whether personal information pertaining to him or her shall be, are being or have been processed
    b. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable
    c. Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information of the controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected
    d. None of the above

17. Statement I: 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
    Statement II: 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
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

18. Statement I: The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosures, as well as against any other unlawful processing
    Statement II: The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

19. Statement I: The employees, agents, or representative of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure
    Statement II: The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

20. Statement I: Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation
    Statement II: The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with the Data Privacy Act. The identify of the individual(s) so designated shall be made known to any data subject upon request
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

21. Statement I: 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
    Statement II: The head of each government agency or instrumentality shall be responsible for complying with the security requirements
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

22. Statement I: 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
    Statement II: Sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

23. Which of the following is not a general data privacy principle?
    a. Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only
    b. Personal information must be disclosed for commercial purposes even without the consent of data subject
    c. Personal information must be processed fairly and lawfully
    d. Personal information must be accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted

24. Which of the following is not a general data privacy principle?
    a. Personal information must be adequate and not excessive in relation to the purposes for which they are collected and processed
    b. Personal information must be processed surreptitiously to achieve the objective of the company
    c. Personal information must be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law
    d. Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed

25. Which of the following is not a criterion for lawful processing of personal information?
    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 in order to take undue advantage on the personal information of the data subject
    d. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject

26. Which of the following is not a criterion for lawful processing of personal information?
    a. The processing is necessary to protect vitally important interests of the data subject, including life and health
    b. 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
    c. The processing pertains to sensitive personal information of the data subject without the consent of the data subject
    d. 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

27. What is the principle about the processing of sensitive personal information and privileged information or communication?
    a. As a general rule, the processing of sensitive personal information and privileged information shall be allowed except to those prohibited by Data Privacy Act
    b. The processing of sensitive personal information and privileged information shall be absolutely prohibited
    c. The processing of sensitive personal information and privileged information shall be absolutely allowed
    d. As a general rule, the processing of sensitive personal information and privileged information shall be prohibited except to those allowed by Data Privacy Act

28. Which of the following is not a right of Data Subject under Data Privacy Act?
    a. Right to question the decision made by the data controller regarding act of management or act of administration of the corporation
    b. Right to be informed whether personal information pertaining to him or her shall be, are being or have been processed
    c. Right to be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity
    d. Right to have reasonable access to, upon demand, the information being processed by the data controller

29. Which of the following is not a right of Data Subject under Data Privacy Act?
    a. Right to dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable
    b. Right to suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected
    c. Right to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information
    d. Right to inspect or access the personal information of other data subject

30. What is the difference between the data privacy and data protection?
    a. Data privacy refers to a person while data protection refers to the technology
    b. Data privacy refers to the technical rules and regulations while data protection refers to substantive laws
    c. Data privacy refers to technology while data protection refers to legal principles
    d. Data privacy refers to the rights of the data subject while data protection refers to the means employed to protects the rights of the data subject

31. This principle means that 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
    a. Transmissibility of rights
    b. Extraterritorial application of Data Privacy Act
    c. Right to data portability
    d. Confidentiality of personal information

32. What is the obligation of National Privacy Commission regarding any personal information that comes to its knowledge and possession?
    a. It shall disclose such personal information without the consent of data subject
    b. It shall sell such personal information for commercial purposes
    c. It shall at all times ensure the confidentiality of such personal information
    d. It shall use such personal information for public persecution

33. Who is National Privacy Commission's head that shall also act as the National Privacy Commission Chairman?
    a. Privacy Chairperson
    b. Privacy Director
    c. Privacy Administrator
    d. Privacy Commissioner

34. Who shall assist the Privacy Commissioner of National Privacy Commission?
    a. Two Assistant Privacy Commissioner, one to be responsible for Data Processing Systems and to be responsible for Policies and Planning
    b. Two Deputy Privacy Commissioner, one to be responsible for Data Processing Systems and to be responsible for Policies and Planning
    c. Two Vice Privacy Commissioner, one to be responsible for Data Processing Systems and to be responsible for Policies and Planning
    d. Two Under Privacy Commissioner, one to be responsible for Data Processing Systems and to be responsible for Policies and Planning

35. Who has the authority to appoint the Privacy Commissioner and the two Deputy Privacy Commissioners?
    a. President of the Republic of the Philippines
    b. Department of Information and Communication Technology (DICT) Secretary
    c. Department of Justice Secretary
    d. Commission of Human Rights (CHR) Chairman

36. What is the term of office of Privacy Commissioner and the two Deputy Privacy Commissioner?
    a. Term of three (3) years and may be reappointed for another term of three (3) years
    b. Term of six (6) years but ineligible for reappointment
    c. Term of seven (7) years but ineligible for reappointment
    d. Term of four (4) years and may be reappointed for another term of four (4) years

37. Which of the following is not a qualification of Privacy Commissioner?
    a. He must be at least 35 years of age
    b. He must be of good moral character, unquestionable integrity and known probity
    c. He must be a recognized expert in the field of information technology and data privacy
    d. He must be a holder of Doctor of Philosophy (PhD) in the field of information technology and data privacy

38. Statement I: The unauthorized processing of personal information shall be penalized by imprisonment ranging from 1 year to 3 years and a fine of not less than P500,000 but not more than P2,000,000 shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized
    Statement II: The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from 3 years to 6 years and a fine of not less than P500,000 but not more than P4,000,000 shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

39. Statement I: The improper disposal of personal information shall be penalized by imprisonment ranging from 6 months to 2 years and a fine of not less than P100,000 but not more than P500,000 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
    Statement II: The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from 1 year to 3 years and a fine of not less than P100,000 but not more than P1,000,000 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
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false

40. Statement I: The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from 1 year and 6 months to 5 years and a fine of not less than P500,000 but not more than P1,000,000 shall be imposed on persons processing personal information for purposes not authorized by the data subject or otherwise authorized
    Statement II: The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from 2 years to 7 years and a fine of not less than P500,000 but not more than P2,000,000 shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized
    a. Only Statement I is true
    b. Only Statement II is true
    c. Both are true
    d. Both are false