Philippine Data Privacy Law

Data Privacy Act of 2012

- In 2012 the Philippines passed the Data Privacy Act 2012, comprehensive and strict privacy legislation "to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth." (Republic Act. No. 10173, Ch. 1, Sec. 2)
- The law applies to the processing of all types of personal information and any legal entity involved in personal information processing
- Companies with at least 250 employees or access to the personal and identifiable information of at least 1,000 people are required to register with the National Privacy Commission and comply with the Data Privacy Act of 2012
- Under **R.A. 10173**, your data is treated almost literally in the same way as your personal property. Thus, it should never be collected, processed, and stored by any organization without your explicit consent, unless otherwise provided by law. Information controllers usually solicit your consent through a consent form. Aside from protecting you against unfair means of personal data collection, this right also requires personal information controllers (PICs) to notify you if your data have been compromised, on time.
- The law requires that when sharing data, the sharing be covered by an agreement that provides adequate safeguards for the rights of data subjects, and that these agreements are subject to review by the National Privacy Commission
- The DPA creates the **National Privacy Commission** ('NPC'), the agency tasked with administering and implementing the provisions of the act, which is headed by a Privacy Commissioner, assisted by two Deputy Commissioners. The NPC has the following powers:
    - Monitor and ensure compliance with the DPA, as well as the rules and regulations implementing its provisions.
    - Receive and resolve complaints and institute investigations.
    - Issue cease and desist orders and impose a temporary or permanent ban on personal information processing.
    - General authority to compel any entity, public or private, to abide by its orders or to take action in a matter affecting data privacy.
    - Recommend the prosecution and imposition of penalties specified in the DPA to the Department of Justice.

Data Controller vs. Data Processor

- The **data controller** has the most responsibility when it comes to protecting the privacy and rights of the **data's subject**, such as the user of a website. Simply put, the data controller controls the procedures and purpose of data usage
- The data controller will be the one to dictate how and why data is going to be used by the organization.
- A **data processor** simply processes any data that the data controller gives them.
    - For instance, Sterling Company has a website that collects data on the pages their visitors visit. This includes the page they enter the site with, the pages that they visited next, and how long they stayed on each page. Sterling Company is the data controller, as they decide how all this information is going to be used and processed, and for what purpose
    - Sterling Company uses Google Analytics to find out which of their pages are most popular and which ones are making Web site visitors leave. This helps them plan their content better by knowing exactly how much time each visitor spends on a particular page. Not only does Sterling Company know which topics to write on, but also discovers new topics that might be of interest to their customers. Plus, it helps them improve on the content that is already there
    - Sterling Company needs to share the data that they get to Google to get the insights they want from Google Analytics. In this case, Google Analytics is the data processor.

- The DPA makes a distinction between personal information controllers and personal information processors, where the former refers to those who decide on the scope of the information collected, including the purpose or extent of its processing, while

the latter refers to those to whom the processing of personal data is outsourced. While processing can be subcontracted, the controller remains responsible for ensuring the confidentiality of data and can be made liable for damages to a data subject, even if the processor was at fault.

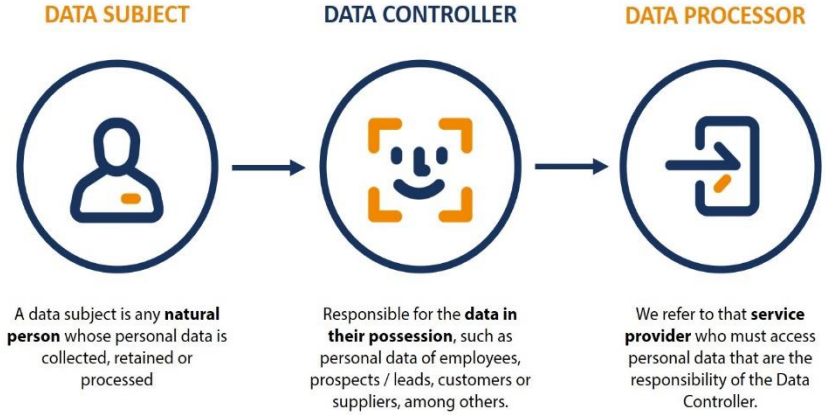

Figure 1. Data Controller and Data Processor

Outsourcing vs. Data Sharing

- The DPA allows the disclosure or transfer of personal data by a personal information controller to a personal information processor for the purposes of **outsourcing** the processing of personal data. The personal information controller must ensure, through contractual or other reasonable means, that proper safeguards necessary for maintaining the confidentiality, integrity, and availability of personal data are in place
- **Data sharing**, on the other hand, refers to an arrangement involving the disclosure of personal data by the controller to a third party.
- Data sharing is allowed as long as the data subject consents and has been provided with specific information regarding the purpose and extent of data sharing, including the intended recipients or categories of recipients of his or her personal data. Consent is required even when the data is to be shared with an affiliate or mother company, or with others of similar relationships. Data sharing for a commercial purpose, including direct marketing, must be covered by a data-sharing agreement, which should establish adequate safeguards for data privacy and security.
    - **Consent** is defined as any freely given, specific, informed indication of will, whereby the data subject agrees to the collection or processing of his or her personal data. This may be evidenced by written, electronic, or recorded means. Consent may also be given on behalf of data subjects by other persons specifically authorized by them.

Data Privacy Law Penalties

- When it comes to the Data Privacy Law, there are different penalties that could be given. The penalty when a business fails to act in accordance with the Data Privacy Law is minimum imprisonment of one (1) year to the maximum of seven (7) years with a fine of not less than One million pesos (Php1,000,000.00) up to Seven million pesos (Php7,000,000.00).
- The penalty can be applied when one of the following has been committed:
    - Unauthorized processing of personal and sensitive information
    - Accessing personal information and sensitive personal information due to negligence
    - Improper disposal of personal information and sensitive personal information
    - Processing of personal information for unauthorized purposes
    - Unauthorized access or intentional breach
    - Concealment of security involving sensitive personal information
    - Malicious disclosure
    - Unauthorized disclosure

References:

Aguda, HR., Tiojanco, BD., Montes, MF. (2017). *Data Privacy & Cybercrime Prevention in the Philippine Digital Age.* Vibal Group.

Dominguez, M. (2018). *A Quick Guide to Philippine Data Privacy Law Compliance.* Clifford Chance.

Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technologies, and regulations.* Addison-Wesley Professional.